PiDuce – a project for experimenting Web services technologies

This is the author's manuscript

Original Citation:
PiDuce – a project for experimenting Web services technologies / Samuele Carpineti; Cosimo Laneve; Luca Padovani. - In: SCIENCE OF COMPUTER PROGRAMMING. - ISSN 0167-6423. - STAMPA. - 74(10)(2009), pp. 777-811.

Availability:
This version is available http://hdl.handle.net/2318/102407 since 2016-11-08T11:54:57Z

Published version:
DOI:10.1016/j.scico.2009.03.002

Terms of use:
Open Access
Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)
PiDuce – a project for experimenting Web services technologies

Samuele Carpineti\textsuperscript{a}, Cosimo Laneve\textsuperscript{a,*}, Luca Padovani\textsuperscript{b}

\textsuperscript{a}University of Bologna, Department of Computer Science, Mura Anteo Zamboni, 7, 40127 Bologna, Italy
\textsuperscript{b}University of Urbino, Information Science and Technology Institute, Piazza della Repubblica, 13, 61029 Urbino, Italy

Abstract

The PiDuce project comprises a programming language and a distributed runtime environment devised for experimenting Web services technologies by relying on solid theories about process calculi and formal languages for XML documents and schemas.

The language features values and datatypes that extend XML documents and schemas with channels, an expressive type system with subtyping, a pattern matching mechanism for deconstructing XML values, and control constructs that are based on Milner’s asynchronous pi calculus. PiDuce programs are compiled into typesafe object code. The runtime environment supports the execution of PiDuce object code over networks by relying on state-of-the-art technologies, such as XML schema and WSDL, thus enabling interoperability with existing Web services.

We thoroughly describe the PiDuce project: the programming language and its semantics, the architecture of the distributed runtime and its implementation. A running prototype is available at http://www.cs.unibo.it/PiDuce/.

Key words: pi calculus, XML schema, type system, subschema relation, WSDL, Web services.

\* Aspects of this investigation were supported in part by a Microsoft initiative in concurrent computing and Web services.
\* Corresponding author.

Email addresses: carpinet@cs.unibo.it (Samuele Carpineti), laneve@cs.unibo.it (Cosimo Laneve), padovani@sti.uniurb.it (Luca Padovani).
1 Introduction

Web services are part of a recent emerging paradigm where computational elements are autonomous, platform-independent and can be described, published, discovered, and orchestrated for developing networks of collaborating applications distributed within and across organizations. Various technologies and languages have been proposed for designing Web services by the major Information Technology vendors. We recall XLANG [33], BizTalk [24], and WS-BPEL [5]. All these languages are informally specified and miss a mathematical model. In fact, they sometime retain vague descriptions of activities (e.g. the execution of compensation handlers in transactional activities), they lack verification tools, and they give poor guarantees about possible implementations.

Process calculi, such as pi calculus [29] and join calculus [16], are possible candidate models for Web services languages. Let us illustrate the point by an example. Consider a book-selling service that accepts requests containing the client identifier and the ordered book. When a request arrives, the book-selling service invokes the services of the Credit and Deposit Departments for verifying the client identity and the book availability. In case of success the request is confirmed, otherwise a failure message is returned. Figure 1 shows a (simplified) description of the book-selling service in WS-BPEL (similar definitions may be given in other Web services process languages such as BizTalk, XLANG, etc.). The format used for this description is XML [28], a widely-used standard for exchanging documents.

The reader familiar with process calculi will recognize the operations of sequence, input (receive), parallel composition (flow), output (invoke), as well as operations that are typical of sequential languages (switch). In particular, ignoring the XML details, the book selling service may be rewritten into a pi calculus-like language as follows:

\begin{verbatim}
OrderPT_in?(BookRequest, ClientId).
  CreditDeptPT_out!(ClientId) | DepositDeptPT_out!(BookRequest)
  \| CreditDeptPT_in?(CreditResponse).
  DepositDeptPT_in?(BookResponse).
  match CreditResponse, BookResponse with
  true, true --> OrderPT_out!("OK")
  _, _ --> OrderPT_out!("NO")
\end{verbatim}

This process and the description of Figure 1 are actually inadequate because they oversimplify the structure of XML documents and the machinery for their parsing. For example lines 3 and 4 in Figure 1 are technically incorrect because the receive element has two attributes with the same name. These lines should be expanded into:
<sequence>
<!--Receive the initial request from client -->
<receive partnerLink="client" portType="com:OrderPT"
operation="BookSelection"
variable="BookRequest" variable="ClientID" />
<!--Make concurrent invocations to Credit \& Deposit Dep-->=  
<flow>
<!--Invoke Deposit Department -->
<invoke partnerLink="DepositDept" portType="ins:DepositDeptPT"
operation="VerifyBookSelection"
inputVariable="BookRequest"
outputVariable="BookResponse" />
<!--Invoke Credit Department -->
<invoke partnerLink="CreditDept" portType="ins:CreditDeptPT"
operation="VerifyCredit" inputVariable="ClientID"
outputVariable="CreditResponse" />
</flow>
<!--verify the responses -->
<switch>
<case condition="getVariableData(BookResponse) == true
&& getVariableData(CreditResponse) == true">
<!--Reply OK to the client -->
<reply partnerLink="client" portType="com:OrderPT"
operation="SelectBook" value="OK" />
</case>
<otherwise>
<!--Reply NO to the Client -->
<reply partnerLink="client" portType="com:OrderPT"
operation="SelectBook" value="NO" />
</otherwise>
</switch>
</sequence>

Fig. 1. A (simplified) description of the book selling service in WS-BPEL.

The above code parses the tree structure of the received XML document, it extracts two fragments located at /BookSelectionInput/BookRequest and /BookSelectionInput/ClientId, and stores such fragments in two variables called BookRequest and ClientId, respectively. Therefore, a process calculus for faithfully describing Web services processes cannot overlook XML values, XML schemas, and patterns.
The PiDuce project (www.cs.unibo.it/PiDuce) aims at developing a calculus of processes that may construct and deconstruct XML documents. The calculus is intended to serve as an intermediate language that is powerful enough to encode the common operations of Web services languages, to assess their expressive power and to develop tools for their analysis. The project also aims at designing a formally specified distributed machine running applications that may be exported to the Web. Overall, PiDuce is not the platform for Web service technologies, but rather it is a formal framework for experimenting proposals, studying their theory, and implementing the relevant features.

The design of the PiDuce language, as well as the prototype implementation, presents some major technical difficulties. The first difficulty regards the treatment of service references. These references are already present in WSDL documents [25], which are the standard files used for publishing and discovering services. Table 2 contains a (simplified) WSDL of the book-selling service.

Recently, a new version of WSDL (WSDL 2.0 [26,27] that, at the time of this writing, is in a Candidate Recommendation status) uses service references in the wsdl:types part of the document. This corresponds to extending types

---
<wsdl:definitions xmlns:tns="http://buy_a_book.com/bookseller/"

targetNamespace="http://buy_a_book.com/bookseller/"
>

<s:element name="BookSelectionRQ">
    <s:sequence>
        <s:element name="BookRequest" type="s:string" />
        <s:element name="ClientId" type="s:string" />
    </s:sequence>
</s:element>

<s:element name="BookSelectionRS" type="s:string" />

<wsdl:operation name="BookSelection">
    <!--the operations of the service -->
    <wsdl:input message="tns:BookSelectionRQ" />
    <wsdl:output message="tns:BookSelectionRS" />
</wsdl:operation>

<wsdl:binding> <!--the locations of the operations -->
    <wsdl:operation name="BookSelection">
        <soap:operation
            soapAction="http://buy_a_book.com/bookseller/BookSelection"/>
    </wsdl:operation>
</wsdl:binding>
</wsdl:definitions>
with service constructors that collect references with a given interface. Therefore, a service invocation may contain a reference that the called service might eventually compare with some local schema before using it. Such a comparison amounts to downloading the schema of the reference and computing a sublanguage relation between schemas. This, in general, requires exponential time in the size of the tree automata of the pattern [14] and may significantly degrade the run-time efficiency of possible implementations. We alleviate this problem by designing a number of restrictions on schemas that make subschema verification polynomial.

A second difficulty regards the implementation. In BizTalk, a service using reliable messaging, such as MSMQ and MQSeries, may receive values from local and remote channels – MessageQueues in BizTalk [24]. For example, the C# fragment below may be obtained in BizTalk by drawing a receive activity on a MSMQ adapter:

```csharp
1. string queueAddress = @"ServerName\QUEUE";
2. MessageQueue q = new MessageQueue(queueAddress, false, false, QueueAccessMode.Receive);
3. Message m = q.Receive();
```

Line 1 defines the address of a queue as consisting of a machine name – the ServerName – and the name of the queue – QUEUE. Line 2 defines a reference q to the address of line 1 specifying the operations that will be performed. In particular, the last argument of MessageQueue constrains the use of q for receiving messages. The receive operation is performed in line 4. This feature is known as input capability in process calculi, which is the mechanism where a received reference is used as the subject of a subsequent input. Implementing input capability in a distributed setting is a hard task because it allows the dynamic creation of large input processes in the wrong place, thus requiring comparatively large code migrations in order to avoid consensus problems. PiDuce admits input capability and implements it by means of linear forwarders [18]. The solution consists of allowing just a limited atom of input capability – the linear forwarder. A linear forwarder is a process that simply turns one message on a Uniform Resource Identifiers (URI) into a message on another. For instance

```
uri1?(m) uri2!(m)
```

is a linear forwarder. To illustrate how linear forwarders enable input capability, consider the process `uri1?(u) u?(v) P`, where P is a continuation process. This process is encoded as

```
uri1?(u) new w in ( spawn { u?(m) w!(m) } w(v) Q )
```

where the input `u?(v)` has been turned into an input `w?(v)` on a service
reference \( u \) \textit{created at the same location as} \( \text{uri} \), and where the forwarder allows one output on \( u \) to interact with \( w \) instead. The key observation is that the linear forwarder is easy to implement: it is just a small message containing two URLs and directed to the location of \( u \). This paper may be also seen as a formal (alternative) implementation of input capability in \textit{BizTalk}, whose implementation details have not been published.

A third difficulty regards \textit{interoporability}. This feature is a primary focus of the \textit{PiDuce} project for two reasons. First of all, it allows us to carry on actual experiments, by letting \textit{PiDuce} define and interact with real Web services. Second, it connects a formally specified system with the current technologies, thus providing such technologies with a foundational basis and possibly spotting their weaknesses, ambiguities, and lines of extension. As an example, a \textit{PiDuce} program should be able to interoperate with the service in Figure 1. In order to do so, it can only rely on the public description of the service – its \textit{WSDL} in Figure 2. A \textit{PiDuce} client for the book-selling service written in \textit{PiDuce} must import the corresponding \textit{WSDL} to ensure that the channels used for communication with the service are typed in accordance with what declared in the client. Symmetrically, a Web service implemented in \textit{PiDuce} must be able to export its operations by means of a \textit{WSDL} resource. Overall, such import/export procedures entail a mapping between the \textit{PiDuce} schemas and, say, XML schema, which is the language typically used in \textit{WSDL} resources to describe the valid documents exchanged with a Web service. This mapping is problematic because the two systems do not have the same expressive power. For example, in \textit{PiDuce} service references are first-class values; therefore \textit{PiDuce} schemas include channel types, which are not supported in XML schema. More generally, \textit{PiDuce} schema retain features that are fundamental in order to guarantee the typability of processes (\textit{cf.} nondeterministic unions of schemas) but which are not found in XML schema. It turns out that the effort for making \textit{PiDuce} interoperable is considerable because what is theoretically clean and well-founded is not necessarily what the technologies provide or what is practically widespread. In this respect the contribution of \textit{PiDuce} is original in that all the exiting languages and distributed machines either lack a formal foundation or are mostly isolated, without a strong connection with actual technologies.

The paper is structured as follows. Section 2 is an introduction to the \textit{PiDuce} language constructs through examples. Section 3 defines the syntax of the language. Section 4 defines the subschema relation and the static semantics of the \textit{PiDuce} process language. Section 5 describes the pattern matching and the operational semantics of local operations. Section 6 defines the \textit{PiDuce} distributed machine and the static and dynamic semantics of operations that deal with remote locations. In Section 7 we close the gap between \textit{PiDuce} and Web service technologies by adding the notions of synchronous communication and service operations. Section 8 briefly describes the architecture of the
PiDuce runtime and shows how PiDuce is interoperable. Section 9 discusses related works and Section 10 concludes with an example of PiDuce program that interoperates with real-world Web services. Appendixes A and B contain proofs of the results stated in the paper. Appendix C presents an algorithmic version of the subschema relation.

2 Getting started

The basic elements of PiDuce are introduced through a few examples. The formal presentation is deferred to the next section.

PiDuce values represent XML documents. For example, the XML document

```xml
<msg>hello</msg><doc/>
```

is written in PiDuce as msg["hello"],doc[ ].

PiDuce schemas are used to type values and approximate XML-Schemas. For example, the XML-Schema

```xml
<xsd:element name="a" type="xsd:integer"/>
```

describing a-labelled integers is written as a[int]. The XML-Schema

```xml
<xsd:element name="a" type="xsd:integer"/>
<xsd:choice>
  <xsd:element name="b" type="xsd:string"/>
  <xsd:element name="c"/>
</xsd:choice>
</xsd:sequence>
```

is written as a[int],(b[string] + c[ ]). Schemas with a repeated structure are written in PiDuce by means of the star operator. For example, the XML-Schema

```xml
<xsd:sequence minOccurs="0" maxOccurs="unbound">
  <xsd:element name="a" type="xsd:string"/>
</xsd:sequence>
```

is written as a[string]*. A detailed discussion of the relationship between XML and PiDuce schemas is undertaken in Section 8.

PiDuce processes describe Web services. For example, a printer service that collects color and black-white printing requests is defined by
print?*(x : Pdf + J Peg)
  match x with {
    y : Pdf => printbw!(y)
    | z : J Peg => printc!(z) }

The print service accepts a value x of schema Pdf + J Peg (where “+” denotes schema union), it checks whether the received value x belongs to either Pdf or J Peg; in the first case it forwards the value x to the black-white printer, in the second case it forwards the value x to the color printer. The basic mechanism for interactions is message passing. For example print!(document) invokes the service print with the value document. Service invocation is non-blocking and asynchronous: the sender does not wait that the receiver really consumes the message. The star after the question mark in the print service above indicates that the service is permanent: the process is capable of handling an unlimited number of requests.

The parallel execution of several activities is defined by the spawn construct. For example

  spawn { print!(document1) } print!(document2)

invokes print twice. Because of asynchrony, there is no guarantee as to which invocation will be served first. More elaborated forms of control and communication, such as sequentiality and rendez-vous, can be encoded using explicit continuation-passing style.

In PiDuce it is possible to select one input out of many. This operation, which is similar to the homonymous system call in socket programming, to the “pick activity” in WS-BPEL, and to the input-guarded choice in the pi calculus, permits the definition of alternative activities. For example, consider a printer service that after the printer request waits for the black-white or color request and prints the document accordingly:

print?*(x : Pdf + J Peg)
select { b&w?( () ) printbw!(x)
         color?( () ) printc!(x) }

(note the missing * after b&w? and color?). In general, the select operation groups several input operations to be executed in mutual exclusion.

Service names may be created dynamically. In their simplest form, services have exactly one operation whose name coincides with that of the service. Services are declared as follows:

new print: (Pdf + J Peg)^0 in P

The new operation creates a new channel at the URL address of the runtime environment executing this code (each service URL is made unique by append-
ing an appropriate suffix) and publishes a WSDL document describing print as an asynchronous – one-way, in WSDL jargon – service (the capability is “O”) accepting documents of schema Pdf + Jpeg. The scope of the declaration is restricted to P. In PiDuce channels are first-class citizens: they are values that can be sent over and received from other channels and they can be examined by pattern matching. With this standpoint, the operation new is intended to declare the schema of a channel literal. Multi-operation services may be also defined. For example the code

```
new cell: {get : ⟨⟨int⟩⟩O; set : ⟨int⟩O} in P
```

defines a service cell with the operations get and set (see Section 7). These operations may be addressed in P by cell#get and cell#set, respectively.

### 3 The PiDuce language

The syntax of PiDuce includes the categories labels, expressions, schemas, patterns, and processes that are defined in Table 1. The following countably infinite sets are used: the set of tags, ranged over by a, b, . . . ; the set of variables, ranged over by x, y, z, . . . ; the set of schema names, ranged over by U, V, . . . ; the set of pattern names, ranged over by Y, J, . . . . Among variables we distinguish channels, i.e. names to be used as URLs, ranged over by u, v, . . . .

A PiDuce program is

```
U_1 = S_1 ; ; ; U_n = S_n ; ; Y_1 = F_1 ; ; ; ; ; ; Y_m = F_m ; ; P
```

that is a sequence of schema and pattern name definitions and a process. For simplicity we assume that the names U_1, . . . , U_n, Y_1, . . . , Y_m are pairwise different. Sequences of schema name and pattern name definitions are represented by maps with finite domain E and F that take a name and return the associated schema or pattern, respectively.

The sets fv(·) of free variables and bv(·) of bound variables are defined for expressions, patterns, and processes as follows:

- fv(E) is the set of variables occurring in E; bv(E) is empty;
- fv(F) is the set of variables occurring in F and, recursively, in the definition of every pattern name occurring in F; bv(F) is empty;
- fv(P) is the set of variables occurring in P that are not bound. An occurrence of x in P is bound in a branch u?(F) P of a select or in the replicated input u?*(F) P if x ∈ fv(F); an occurrence of u in P is bound in new u: ⟨S⟩κ in P.
- bv(P) collects the bound variables in P.
Table 1

**PiDuce syntax (B includes int, string, integer and string constants).**

<table>
<thead>
<tr>
<th>$L ::= $</th>
<th>label</th>
<th>$F ::= $</th>
<th>pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>(tag)</td>
<td>$\emptyset$</td>
<td>(void pattern)</td>
</tr>
<tr>
<td>$\sim$</td>
<td>(wildcard label)</td>
<td>$B$</td>
<td>(basic schema)</td>
</tr>
<tr>
<td>$L + L$</td>
<td>(union)</td>
<td>$\langle S \rangle^c$</td>
<td>(channel pattern)</td>
</tr>
<tr>
<td>$L \setminus L$</td>
<td>(difference)</td>
<td>$S^c$</td>
<td>(star pattern)</td>
</tr>
</tbody>
</table>

$E ::= $ expression

| $()$ | (void) |
| $n$ | (integer constant) |
| $s$ | (string constant) |
| $x$ | (variable) |
| $a[E]$ | (labelled expression) |
| $E, E$ | (sequence) |

$S ::= $ schema

| $()$ | (void schema) |
| $B$ | (basic schema) |
| $\langle S \rangle^c$ | (channel schema) |
| $L[S]$ | (labelled schema) |
| $S, S$ | (sequence schema) |
| $S + S$ | (union schema) |
| $S^c$ | (star) |
| $U$ | (schema name) |

$F ::= $ pattern

| $x : F$ | (variable binder) |
| $L[F]$ | (labelled pattern) |
| $F, F$ | (sequence pattern) |
| $F + F$ | (union pattern) |
| $Y$ | (pattern name) |

$P ::= $ process

| $0$ | (nil) |
| $u! E$ | (output) |
| $\text{select } \{ u? (F_i) \ P_i \ i \in 1..n \}$ | (select) |
| $\text{new } u : \langle S \rangle^c \text{ in } P$ | (new) |
| $\text{match } E \text{ with } \{ F_i \Rightarrow P_i \ i \in 1..n \}$ | (match) |
| $u?* (F) \ P$ | (spawn) |

The definitions of alpha-conversion and substitution for bound variables are standard. In the whole paper, we identify terms that are equal up-to alpha-conversion. In the following, the channel $u$ in $u! E$, $u? (F)$ and $u?* (F)$ is called subject.

**Labels.** Labels specify collections of tags. Let $\mathcal{L}$ be the set of all tags; the semantics of labels is defined by the $\sim$ function:

$$\sim = \mathcal{L} \quad L + L' = \hat{L} \cup \hat{L}' \quad L \setminus L' = \hat{L} \setminus \hat{L}'$$

We write $a \in L$ for $a \in \hat{L}$. Label intersection is a derived operator: $L \cap L' \stackrel{\text{def}}{=} \sim \setminus ((\sim \setminus L) + (\sim \setminus L'))$.

**Expressions.** Expressions are the empty sequence $()$, integer and string constants, variables, labelled expressions, or sequences of expressions. The PiDuce prototype also includes primitive operations over basic schemas. The
formal treatment of such operations is omitted as it is standard and not interesting. In the following, whenever possible, \( \emptyset \) is omitted: expressions such as \( a[\emptyset] \) and \( a[E] \), \( \emptyset \) are shortened into \( a[\ ] \) and \( a[E] \), respectively.

Channels are references to services. They represent URL addresses of the corresponding WSDL interfaces, such as http://www.cs.unibo.it/PiDuce.wsdl. Section 8 discusses how WSDL interfaces are related to PiDuce services.

A relevant subset of expressions is that of values, which are the normalized expressions exchanged during communications. As in pi calculus, PiDuce values may contain channels, which are variables. For example \( a[x] \) is a value inasmuch as \( x \) is a channel. Values with variables in a set \( Z \), called \( Z\)-values, are possibly empty sequences of constants, variables in \( Z \), and labelled \( Z\)-values.

In particular, expressions such as \( , a[1] \) or \( a[1], () \), \( b[\text{true}] \) or \( a[1], () \) or \( u \) are not \( \emptyset \)-values. Values are ranged over by \( V, W, \ldots \), and, in the following, the set \( Z \) is omitted when it is clear from the context.

The evaluation function \( \downarrow_Z \), where \( Z \) is a set of variables, turns expressions into values and is defined by the following rules:

\[
\begin{align*}
(\ ) & \downarrow_Z (\ ) \quad n \downarrow_Z n \quad s \downarrow_Z s \\
E & \downarrow_Z V \\
E \downarrow_Z V & = E, E' \downarrow_Z V @ V'
\end{align*}
\]

where the concatenation \( @ \) of two values is defined as follows:

\[
\begin{align*}
(\ ) @ V &= V @ (\ ) = V \\
V @ V' &= V, V' & \text{if } (V = n \text{ or } V = s \text{ or } V = x \text{ or } V = a[V']) \\
&\text{and } V' \neq (\ )
\end{align*}
\]

\[
(V, V') @ V'' = V @ (V' @ V'')
\]

**Schemas.** Schemas describe collections of structurally similar values. The syntax of schemas includes the category of basic types \( B \) that, in this paper, are integers (\texttt{int}), strings (\texttt{string}) and integer and string constants \( n \) and \( s \), respectively. The basic types \( n \) and \( s \) represent the sets \( \{n\} \) and \( \{s\} \), respectively. The schema \( \emptyset \) describes the empty value. The schema \( \langle S \rangle^\kappa \) describes channels that carry messages of schema \( S \) and that may be used with capability \( \kappa \in \{I, O, IO\} \). The capabilities \( I, O, IO \) mean that the channel can be used for performing inputs, outputs, and both inputs and outputs, respectively. For example \( \langle \text{int} \rangle^0 \) describes the set of channels on which it is possible to send integer values. The schema \( L[S] \) describes labelled values whose tag is in \( L \) and containing a value of schema \( S \). The schema \( S, S' \) describes sequences having a prefix of schema \( S \) and the remaining suffix of schema \( S' \). In what follows \( L[()], () , S \) and \( S, () \) are shortened into \( L[ ] \), \( S \), and \( S \), respectively.
The schema $S + S'$ describes the set of values whose schema is either $S$ or $S'$. The schema $S^*$ describes the set of values that are described by every finite (possibly empty) sequence $S, \ldots, S$. Schemas include schema names that are bound by finite maps $E$ from schema names to schemas such that, for every $U \in \text{dom}(E)$, the schema names in $E(U)$ belong to $\text{dom}(E)$. Maps $E$ are well-formed according to the definition below. Let $\text{tls}(S)$ be the least function such that:

$$
\text{tls}(S) = \begin{cases} 
\{U\} \cup \text{tls}(E(U)) & \text{if } S = U \\
\text{tls}(T) & \text{if } S = T^* \\
\text{tls}(T) \cup \text{tls}(T') & \text{if } S = T + T' \text{ or } S = T, T' \\
\emptyset & \text{otherwise}
\end{cases}
$$

Then $E$ is well-formed if, for every $U \in \text{dom}(E)$, $U \not\in \text{tls}(E(U))$. The well-formedness and the finiteness of the domain of $E$ guarantee that PiDuce schemas only define regular tree languages (such languages retain a decidable sublanguage relation, which is a fundamental operation in PiDuce type checking and pattern-matching) [14].

The following definitions will be used in the rest of the paper:

- Empty = ~[Empty] ;;
- AnyChan = ⟨Empty⟩∪⟨Any⟩I ;;
- Any = (int + string + AnyChan + ~[Any])* ;;

The name Empty describes the empty set of values; AnyChan describes any channel; Any describes any value. Empty and Any are respectively the least and the greatest schema according to the subschema relation of Section 4 (Proposition 2(9)).

**Patterns.** Patterns permit the deconstruction of values using matching. The patterns $O$, $B$, $(S)^*$, and $S^*$ match values of the corresponding schemas. The pattern $x : F$ matches the same values matched by $F$ and additionally it binds such values to the variable $x$. The pattern $L[F]$ matches values of the form $a[V]$, when $a \in L$ and $F$ matches $V$. The pattern $F, F'$ matches values $V = V'@V''$ such that $V'$ and $V''$ are matched by $F$ and $F'$, respectively. The pattern $F + F'$ matches values $V$ that are matched by either $F$ or $F'$. The pattern matching algorithm is deterministic:

1. in a pattern $S^*, F$, the partition of $V$ into $V'@V''$ is such that $V'$ is the longest prefix of $V$ that is matched by $S^*$ (longest match policy);
2. in a pattern $F + F'$ the match with the left-hand side pattern is attempted first; in case of failure, the match with the right-hand side pattern is attempted (first match policy).
Patterns include pattern names that are bound by finite maps $\mathcal{F}$ from pattern names to patterns such that, for every $Y \in \text{dom}(\mathcal{F})$, the pattern names in $\mathcal{F}(Y)$ belong to $\text{dom}(\mathcal{F})$. Pattern definitions must obey the same well-formedness restrictions of schema definitions. In addition, PiDuce patterns are linear, namely the following three conditions hold:

1. every pattern $x : F$ is such that $x \notin \text{fv}(F)$;
2. every pattern $F, F'$ is such that $\text{fv}(F) \cap \text{fv}(F') = \emptyset$;
3. every pattern $F + F'$ is such that $\text{fv}(F) = \text{fv}(F')$.

In the following we write $\text{schof}(F)$ for the schema obtained by erasing all the variables in $F$.

Processes. Processes are the computing entities of PiDuce. $0$ is the idle process; $u!(E)$ evaluates $E$ to a value and outputs it on the channel $u$. The process $\text{select} \{u?((F_i) P_i \ i \in 1..n}\}$ inputs a value on the channel $u_i$, matches the value with $F_i$ yielding a substitution $\sigma$ and behaves as $P_i\sigma$. We always abbreviate $\text{select} \{u?(F) P\}$ to $u?(F) P$. The process $\text{new} \ u:\langle S \rangle \ \kappa \ \text{in} \ P$ defines a fresh channel $u$ and binds it within the continuation $P$, where $u$ may be used as subject of input and output operations, whereas the capability $\kappa$ is exposed in the WSDL interface associated with the channel (see Section 8). The process $\text{match} E \ \text{with} \ \{F_i \Rightarrow P_i \ i \in 1..n\}$ tests whether the value to which $E$ evaluates is matched by one of the patterns $F_i$’s. The order of the branches is relevant, so that the first matching pattern determines the continuation (first match policy). If the match with $F_k$ succeeds, the continuation $P_k\sigma$ is run, where $\sigma$ is the substitution yielded by the pattern matching algorithm. The process $\text{spawn} \ \{P\} Q$ spawns the execution of $P$ on a separate thread and continues as $Q$. The replicated input $u?\ast(F) P$ consumes a message on $u$, it spawns the continuation $P\sigma$, where $\sigma$ is the substitution yielded by matching the message with the pattern $F$, and then it becomes available for other messages on $u$.

The syntax of Table 1 will be extended in Section 6 with operations regarding remote machines, such as the creation of channels at remote locations or the select on remote channel.

4 The subschema relation and the type system

A basic check in the PiDuce compiler and runtime is the language containment of schemas, called subschema relation. In [21] this notion is defined in terms of set-containment. In particular, let $[S] \overset{\text{def}}{=} \{V \mid V \text{ is of schema } S\}$. Then $S$ is a subschema of $T$ if $[S] \subseteq [T]$. This approach is inadequate in PiDuce because
of the presence of channels. Indeed, the values of $\langle S \rangle^0$ are sets of names that may be defined at runtime. To circumvent this problem we follow an approach proposed in [4] and already used in pi calculus [31].

Let $S \downarrow R$, read $S$ has handle $R$, be the least relation such that:

- $\emptyset \downarrow \emptyset$
- $B \downarrow B, ()$
- $\langle S \rangle^* \downarrow \langle S \rangle^*, ()$
- $L[S] \downarrow L[S], ()$ if $L \neq \emptyset$ and, for some $R$, $S \downarrow R$
- $S, S' \downarrow R$ if $S \downarrow ()$ and $S' \downarrow R$
- $S, S' \downarrow R, S'$ if $S \downarrow R$ and $R \neq ()$ and, for some $R'$, $S' \downarrow R'$
- $S + S' \downarrow R$ if $S \downarrow R$ or $S' \downarrow R$
- $\cup \downarrow R$ if $E(\cup) \downarrow R$
- $S^* \downarrow ()$
- $S^* \downarrow R, S^*$ if $S \downarrow R$ and $R \neq ()$

The relation “$\downarrow$” singles out the branches of the syntax tree of a schema. For example $(a[\text{int}], \text{string} + b[\text{string}], \text{int}) \downarrow a[\text{int}], \text{string}$. We observe that $\text{Empty}$ has no handle. The schema $a[\text{int}], \text{Empty}$ has no handle as well; the reason is that a sequence has a handle provided that every element of the sequence has a handle. We also remark that a channel $\langle S \rangle^\kappa$ always retains a handle. Let $S$ be not-empty if and only if $S$ has a handle; it is empty otherwise.

**Definition 1** Let $\leq$ be the least partial order on capabilities such that $\text{IO} \leq I$ and $I, \emptyset \leq 0$. Let $\sqsubseteq$ be the least partial order on basic schemas such that $n \sqsubseteq \text{int}$ and $s \sqsubseteq \text{string}$. A subschema $R$ is a relation on schemas such that $S R T$ implies:

1. $S \downarrow ()$ implies $T \downarrow ()$;
2. $S \downarrow B, S'$ implies $T \downarrow B_i, T_i'$, for $1 \leq i \leq n$, with $B \sqsubseteq B_i$ and $S' \sqsubseteq \sum_{1 \leq i \leq n} T_i'$;
3. $S \downarrow \langle S \rangle^\kappa, S''$ implies $T \downarrow \langle T_i \rangle^\kappa, T_i'$, for $1 \leq i \leq n$, with $\kappa \leq \kappa_i$, $S'' \sqsubseteq \sum_{1 \leq i \leq n} T_i'$, and, for every $1 \leq i \leq n$, one of the following conditions holds:
   - (a) $\kappa_i = 0$ and $T_i' \sqsubseteq S'$, or
   - (b) $\kappa_i = 1$ and $S' \sqsubseteq T_i'$, or
   - (c) $\kappa_i = \text{IO}$ and $S' \sqsubseteq T_i'$ and $T_i' \sqsubseteq S'$;
4. $S \downarrow L[S'], S''$ implies that one of the following conditions holds:
   - (a) $T \downarrow L', T''$ with $\hat{L} \cap \hat{L}' = \emptyset$, $\hat{L} \nsubseteq \hat{L}'$, $(L \setminus L') \langle S \rangle^\kappa, S'' \sqsubseteq \sum_{1 \leq i \leq n} T_i'$, and $(L \setminus L') \langle S \rangle^\kappa, S'' \sqsubseteq T$, or
   - (b) $T \downarrow L_i[T_i], T_i'$, for $1 \leq i \leq n$, with $\hat{L} \subseteq \cap_{i \in \{1, \ldots, n\}} \hat{L}_i$ and, for every $J \subseteq \{1, \ldots, n\}$, either $S' \sqsubseteq \sum_{i \in J} T_i$ or $S'' \sqsubseteq \sum_{i \in \{1, \ldots, n\} \setminus J} T_i$.

Let $\preceq$: be the largest subschema relation.
The definition of subschema is commented upon below. Item 1 constraints greater schemas to manifest a void handle if the smaller one retains such a handle. Item 2 deals with basic schemas $B, S'$; a set of handles $B_i, T'_i$ of the greater schema is selected such that $B$ is smaller than $B_i$ and $S'$ is smaller than the union of the $T'_i$’s. Item 3 is similar to item 2, except for the heads of handles, which are channel schemas. In order to check the subschema relation between $(S)^{\kappa}$ and $(T)^{\kappa}$, the capability $\kappa$ must be smaller than $\kappa'$. Additionally, in case $\kappa' = 0$ the subschema is inverted on the arguments (contravariance); in case $\kappa' = 1$ the subschema is the same as for the arguments (covariance), in case $\kappa' = \emptyset$ the relation reduces to check the equivalence of the arguments (invariance). For example $(\text{int} + \text{string})^0 <: (\text{int})^0$ because every channel that may carry either integers or strings can carry integers only. On the contrary, $(\text{int})^1 <: (\text{int} + \text{string})^1$ because every channel that may serve invocations carrying either integers or strings can serve invocations with integers only.

Item 4 is the most complex one. It deals with handles $L[S'], S''$. We illustrate the point by means of an example. The case (a) accounts for subschema relations between $S = (a + b)[\text{int}], \text{int}$ and $T = a[\text{int}], b[\text{int}], \text{int}$. Since $T \downarrow a[\text{int}], \text{int}$, according to 4.a, the relation may be reduced to the check whether $((a+b)\backslash a)[\text{int}], \text{int}$ and $((a+b)\cap a)[\text{int}], \text{int}$ are subschema of $T$. The case (b) accounts for subschema relations between $S = a[\text{int} + \text{string}], \text{int}$ and $T = a[\text{int}], a[\text{string}], \text{int}$. We explain this case by using an argument similar to that used in [22]. Let us admit a schema intersection operator $\cap$ such that $S \cap T$ describes the values that belong to both $S$ and $T$. Then $L[S], T$ may be rewritten as $L[S], \text{Any} \cap \text{~Any}, T$ using the fact that $\text{Any}$ is the greatest schema (see Proposition 2.6). Then:

$$L_1[S_1], T_1 + L_2[S_2], T_2 = (L_1[S_1], \text{Any} \cap \text{~Any}, T_1) + (L_2[S_2], \text{Any} \cap \text{~Any}, T_2)$$

$$= (L_1[S_1], \text{Any} + L_2[S_2], \text{Any}) \cap (\text{~Any}, T_1 \cap \text{~Any}, T_2)$$

$$\cap (L_1[S_1], \text{Any} + \text{~Any}, T_2) \cap (\text{~Any}, T_1 + L_2[S_2], \text{Any})$$

where the last equality follows by distributivity of $\cap$ with respect to union. Therefore, if one intends to derive that $L[S], T$ is a subschema of $L_1[S_1], T_1 + L_2[S_2], T_2$ when $\hat{L} \subseteq \hat{L}_1 \cap \hat{L}_2$, it is possible to reduce to:

for every $J \subseteq \{1, 2\}$ either $S \mathcal{R} \sum_{j \in J} S_j$ or $T \mathcal{R} \sum_{j \in \{1, 2\} \setminus J} T_j$

This is exactly item 4.b when $I = \{1, 2\}$. A particular case is when $I = \{1\}$. For example verifying that $a[S], T$ is a subschema of $(a+b)[S'], T'$. In this case the subsets of $I$ are $\emptyset$ and $\{1\}$ and one is reduced to prove (we let $\sum_{j \in \emptyset} S_j =$ Empty):

$$\left( S \mathcal{R} \text{Empty} \text{ or } T \mathcal{R} T' \right) \text{ and } \left( S \mathcal{R} S' \text{ or } T \mathcal{R} \text{Empty} \right)$$

15
That is, when $S$ and $T$ are not subschema of $\text{Empty}$, we are reduced to $S \mathcal{R} S'$ and $T \mathcal{R} T'$.

The schemas $\text{AnyChan}$ and $\text{Any}$ own relevant properties. $\text{AnyChan}$ collects all the channel schemas, no matter what they can carry; $\text{Any}$ collects all the values, namely possibly empty sequences of possibly labelled values, including channels. We observe that $\langle \text{Empty} \rangle^0$ and $\langle \text{Any} \rangle^0$ are very different. $\langle \text{Empty} \rangle^0$ collects every channel with either capability “0” or “10”; $\langle \text{Any} \rangle^0$ refers only to channels where arbitrary data can be sent. For instance $\langle a[] \rangle^0$ is a subschema of $\langle \text{Empty} \rangle^0$ but not of $\langle \text{Any} \rangle^0$. The channel schemas $\langle \text{Any} \rangle^1$ and $\langle \text{Empty} \rangle^1$ are different as well. $\langle \text{Any} \rangle^1$ refers to references that may receive arbitrary data; $\langle \text{Empty} \rangle^1$ refers to a reference that cannot receive anything.

A few properties of $\langle \cdot \rangle^+$ are in order. The proofs can be found in Appendix A.

**Proposition 2**

1. $\langle \cdot \rangle^+$ is reflexive and transitive;
2. If $S$ is empty, then $S <: \text{Empty}$;
3. (Contravariance of $\langle \cdot \rangle^0$) $S <: T$ if and only if $\langle T \rangle^0 <: \langle S \rangle^0$;
4. (Covariance of $\langle \cdot \rangle^1$) $S <: T$ if and only if $\langle S \rangle^1 <: \langle T \rangle^1$;
5. (Invariance of $\langle \cdot \rangle^{10}$) $S <: T$ and $T <: S$ if and only if $\langle S \rangle^{10} <: \langle T \rangle^{10}$;
6. If $S <: T$, then $S,() <: T$; if $(),S <: T$, then $S <: T$;
7. If $S <: T$ and $S' <: T'$, then $S,S' <: T,T'$;
8. If $(S+S'),S'' <: T$, then $S,S' <: T$ and $S',S'' <: T$;
9. For every $S$, $\text{Empty} <: S <: \text{Any}$ and $\langle S \rangle^* <: \text{AnyChan}$ and $\langle \text{Any} \rangle^{10} <: \langle S \rangle^0$ and $\langle \text{Empty} \rangle^{10} <: \langle S \rangle^1$.

**Remark 3** The algorithm for computing the subschema relation in PiDuce is similar to the one developed for XDuce [22]. It is computationally expensive: the cost of the algorithm for subschema is exponential in the size of the schemas. Paying this cost at compile time may be acceptable. However, in PiDuce the subschema relation is invoked at runtime by pattern matching (see Section 5). Paying an exponential cost at runtime becomes fateful because the performance degradation might be unacceptable. For instance an attacker might block a service by invoking it with channels of complex schemas, thus yielding a denial of service. A set of constraints on schemas that reduce the cost of the subschema algorithm has been designed in [11]. The PiDuce compiler warns the user when programs use schemas that do not meet such constraints. We defer this issue to Appendix C.

### 4.1 The PiDuce type system

Few preliminary notations are introduced. Let $\Gamma$, $\Delta$, called environments, be finite maps from variables to schemas. We write $\text{dom}(\Gamma)$ for the set of names in the domain of $\Gamma$. Let $\Gamma + \Delta$ be $(\Gamma \setminus \text{dom}(\Delta)) \cup \Delta$, where $\Gamma \setminus X$ removes from $\Gamma$ all
Expressions:

\[ \begin{align*}
& \Gamma \vdash O : O \quad \Gamma \vdash n : n \quad \Gamma \vdash s : s \\
& \Gamma(x) = S \\
& \Gamma \vdash x : S \\
& a \in L \quad \Gamma \vdash E : S \\
& \Gamma \vdash a[E] : L[S] \\
& \Gamma \vdash E, E' : S, S' \\
\end{align*} \]

Processes:

\[ \begin{align*}
& (\text{NIL}) \quad \Delta \vdash 0 \\
& (\text{OUT}) \quad \Gamma ; \Delta \vdash E : S \quad \Gamma \vdash u : T \quad T \ll : \langle S \rangle^0 \\
& \Gamma ; \Delta \vdash u ! (E) \\
& (\text{NEW}) \quad \Gamma + u : \langle S \rangle^c ; \Delta + u : \langle S \rangle^0 \vdash P \\
& \Gamma ; \Delta \vdash \text{new } u : \langle S \rangle^c \text{ in } P \\
& (\text{MATCH}) \quad \Gamma + \Delta \vdash E : S \quad ((\Gamma ; \Delta) + \text{Env}(F_i) \vdash P_i)_{i \in 1..n} \\
& S \ll : \sum_{i \in 1..n} \text{schof}(F_i) \\
& \Gamma ; \Delta \vdash \text{match } E \text{ with } \{ F_i \Rightarrow P_i \}^{i \in 1..n} \\
& (\text{SPAWN}) \quad \Gamma ; \Delta \vdash P \quad \Gamma ; \Delta \vdash P' \\
& \Gamma ; \Delta \vdash \text{spawn } \{ P \} \quad \Delta \vdash u : S \quad (\Gamma ; \Delta) + \text{Env}(F) \vdash P \\
& S \ll : \langle \text{schof}(F) \rangle^1 \\
& \Gamma ; \Delta \vdash u ? *(F) P \\
& (\text{REPIN}) \quad \Gamma ; \Delta \vdash P \quad \Gamma ; \Delta \vdash P' \\
& Length the bindings of names in X. Let also (\Gamma ; \Delta) + \Gamma' be the pair \Gamma + \Gamma' ; \Delta \setminus \text{dom}(\Gamma'). Finally, let Env(.) be the least function such that:

\[ \begin{align*}
& \text{Env}(S) = \emptyset \\
& \text{Env}(u : F) = u : \text{schof}(F) + \text{Env}(F) \ (u \not\in \text{dom}(\text{Env})(F)) \\
& \text{Env}(L[F]) = \text{Env}(F) \\
& \text{Env}(F, F') = \text{Env}(F) + \text{Env}(F') \quad (\text{dom}(\text{Env})(F) \cap \text{dom}(\text{Env})(F') = \emptyset) \\
& \text{Env}(F + F') = \text{Env}(F) \\
& \text{Env}(Y) = \text{Env}(F(Y)) \\
\end{align*} \]

The judgments \( \Gamma \vdash E : S \) – read \( E \) has schema \( S \) in the environment \( \Gamma \) – and \( \Gamma ; \Delta \vdash P \) – read \( P \) is well typed in the environment \( \Gamma \) and local environment \( \Delta \) – are the least relations satisfying the rules in Table 2.

Rules for expressions, (NIL) and (SPAWN) are standard. Rule (OUT) types outputs. By definition of subschema, the premise \( T \ll : \langle S \rangle^0 \) entails that \( u \) may carry messages of schema \( S \). We note that \( u \) can be typed as a union of channel schemas, for example \( u : \langle a[\text{int}] + () \rangle^0 + \langle b[\text{string}] + () \rangle^0 \). When this is the
case, $E$ must be a subschema of every schema carried by $u$. In this example, the unique possible schema for $E$ is (). Rule (SELECT) types input-guarded choices. The first hypothesis types subjects. The second hypothesis types the continuation of every summand in the environment $\Gamma; \Delta$ plus that defined by the pattern. The third hypothesis checks the exhaustiveness of every pattern. As for outputs the hypothesis $S_i <: \langle \text{schof}(F_i) \rangle^I$ does not strictly require $u_i$ to be a channel schema. Rule (NEW) types new $u : \langle S \rangle^\kappa$ in $P$ in $\Gamma; \Delta$ provided that $P$ is typable with in $\Gamma + u : \langle S \rangle^\kappa; \Delta + u : \langle S \rangle^{10}$. The first component of the pair of environments is extended with the exported schema $\langle S \rangle^\kappa$ of the channel; this definition is used for typing expressions to be sent as messages (see rule (OUT)). The second component is extended with the internal schema of the channel $\langle S \rangle^{10}$; this definition is used for typing subjects of inputs and outputs (see rules (OUT), (SELECT), and (REPIN)). Rule (MATCH) derives the typing of match $E$ with $\{F_i \Rightarrow P_i\}_{i=1..n}$ provided $E$ and $P_i$ are well typed in the environments $\Gamma + \Delta$ and $(\Gamma; \Delta) + \text{Env}(F_i)$, respectively. The third hypothesis checks the exhaustiveness of patterns with respect to the schema of $E$. Rule (REPIN) is similar to (SELECT) but the subject is checked to be local.

Remark 4 The PiDuce compiler also verifies whether patterns in match operators are redundant. In particular in rule (MATCH) the compiler verifies that, for every $1 \leq i \leq n - 1$, $\text{schof}(F_i) <: S$ and, for every $2 \leq j \leq n$, $\text{schof}(F_j) \not<: \sum_{k<j} \text{schof}(F_j)$. In case, the user is warned with suitable messages.

5 Pattern matching and local operational semantics

This section defines the semantics of patterns and processes. In order to cope with values that may carry channels, both the pattern matching and the transition relation take an associated environment into account. As regards processes, this section details the semantics of operations that are performed by a single PiDuce runtime environment. The operations retaining a distributed semantics are discussed in Section 6.

5.1 Pattern matching

Let $\sigma$ and $\sigma'$ be two substitutions with disjoint domains. We write $\sigma + \sigma'$ to denote the substitution that is the union of $\sigma$ and $\sigma'$. Every union in the following rules is always well defined because of the linearity constraint on patterns. Let a marker be an object of the form $x/V$; let $\Phi$ be a possibly empty sequence of patterns or markers separated by $::$ and let $[\ ]$ be the empty
Table 3
Pattern matching rules.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(pm1)</td>
<td>$\Delta \vdash \emptyset \in [\ ] \sim \emptyset$</td>
</tr>
<tr>
<td>(pm2)</td>
<td>$\Delta \vdash V \in \Phi \sim \sigma \quad \frac{\Delta \vdash V \in \emptyset}{\Delta \vdash \emptyset : \Phi \sim \emptyset}$</td>
</tr>
<tr>
<td>(pm3)</td>
<td>$\Delta \vdash V \in \Phi \sim \sigma \quad V = V''@V \quad \frac{\Delta \vdash V \in x/V' : \Phi \sim \emptyset + [x \leftarrow V'']}{\Delta \vdash \emptyset : x/V' : \Phi \sim \emptyset}$</td>
</tr>
<tr>
<td>(pm4)</td>
<td>$b &lt;: B \quad \Delta \vdash b@V \in B : \Phi \sim \sigma \quad \frac{\Delta \vdash b@V \in B : \Phi \sim \sigma}{\Delta \vdash \emptyset : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm5)</td>
<td>$\Delta(u) &lt;: S \quad \Delta \vdash u@V \in S : \Phi \sim \sigma \quad \frac{\Delta \vdash u@V \in S : \Phi \sim \sigma}{\Delta \vdash \emptyset : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm6)</td>
<td>$a \in L \quad \Delta \vdash V \in F \sim \sigma \quad \Delta \vdash V' \in \Phi \sim \sigma' \quad \frac{\Delta \vdash V \in (F + F') : \Phi \sim \sigma + \sigma'}{\Delta \vdash a[V]@V' \in L[F] : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm7)</td>
<td>$\Delta \vdash V \in F : x/V' : \Phi \sim \sigma \quad \frac{\Delta \vdash V \in F : \Phi \sim \sigma}{\Delta \vdash \emptyset : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm8)</td>
<td>$\Delta \vdash V \in F : \Phi \sim \sigma \quad \frac{\Delta \vdash V \in (F + F') : \Phi \sim \sigma}{\Delta \vdash V \in F : \Phi \sim \sigma + \sigma'}$</td>
</tr>
<tr>
<td>(pm9)</td>
<td>$\Delta \vdash V \not\in F' : \Phi \sim \sigma \quad \frac{\Delta \vdash V \in (F + F') : \Phi \sim \sigma}{\Delta \vdash V \not\in F : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm10)</td>
<td>$\Delta \vdash V \in F : F' : \Phi \sim \sigma \quad \frac{\Delta \vdash V \in (F,F') : \Phi \sim \sigma}{\Delta \vdash V \in F : F' : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm11)</td>
<td>$\Delta \vdash V \in F(Y) : \Phi \sim \sigma \quad \frac{\Delta \vdash V \in Y : \Phi \sim \sigma}{\Delta \vdash V \in F(Y) : \Phi \sim \sigma}$</td>
</tr>
<tr>
<td>(pm12)</td>
<td>$\Delta \vdash V \in S^n \sim \emptyset \quad \Delta \vdash V' \in \Phi \sim \sigma \quad (V' = W@V'' \text{ and } W \neq \emptyset) \implies (\Delta \vdash V@W \not\in S* \text{ or } \Delta \vdash V'' \not\in \Phi) \quad \frac{\Delta \vdash V@V' \in S^n : \Phi \sim \sigma}{\Delta \vdash \emptyset : \Phi \sim \sigma}$</td>
</tr>
</tbody>
</table>

The pattern matching of a value $V$ with respect to a sequence $\Phi$ in an environment $\Delta$, written $\Delta \vdash V \in \Phi \sim \sigma$, is defined by the rules in Table 3. We write $\Delta \vdash V \in \Phi$ if there exists $\sigma$ such that $\Delta \vdash V \in \Phi \sim \sigma$; we write $\Delta \vdash V \not\in \Phi$ if not $\Delta \vdash V \in \Phi$. Let $S^n$ be $S, \ldots, S$ with $n$ repetitions of $S$; let $S^0$ be $\emptyset$.

Rule (pm1) matches $\emptyset$ with the empty sequence. This rule must be read in conjunction with (pm2), which removes void patterns in head position of sequences. Rule (pm3) defines markings. A marking $x/V'$ is inserted in $\Phi$ by patterns $x : F$—see rule (pm7); it records the value $V'$ that must be matched by $\Phi$ when a variable binder is found. The rule binds $x$ to the prefix of $V'$ that has been matched by $F$. Rule (pm4) matches constants with basic schemas. Rule (pm5) matches channels with patterns that do not contain variables and, assuming that $\Delta(u)$ is a channel schema, that are greater than a channel schema. Rule (pm6) deals with labelled values. Rule (pm7) defines the pattern matching of a sequence $(x : F) : \Phi$. In this case, the value $V$ must match
with $F \colon \Phi$ and the prefix of $V$ matching with $F$ must be bound to $x$. This is the purpose of the marking that is inserted between $F$ and $\Phi$. Rules (PM8) and (PM9) define the pattern matching for union patterns. They implement the first match policy: in a pattern $F + F'$ the match with $F$ is attempted and, if this fails, the match with $F'$ is tried. Rule (PM10) turns sequence patterns into sequences $\Phi$. Rule (PM11) defines pattern matching of pattern names in the obvious way. Finally, rule (PM12) defines the pattern matching for $S^* \colon \Phi$ sequences. The pattern $S^*$ is equal to the choice $() + S + (S, S) + (S, S, S) + \cdots$ but it is managed by a policy different than the one of rules (PM8) and (PM9). In this case the standard policy is the longest match one: a partition $V@V'$ of the value is looked for such that $V$ is the longest prefix matching with $S^*$ and $V'$ is a suffix matching with $\Phi$.

Rules (PM8), (PM9), and (PM12) make the parsing for patterns $F + F'$ and $S^*$ deterministic. The pattern matching of Table 3 is therefore unambiguous.

**Proposition 5** If $\Delta \vdash V \in \Phi$ then there exists a unique $\sigma$ such that $\Delta \vdash V \in \Phi \leadsto \sigma$.

Notwithstanding this unicity property, the implementation of the pattern matching algorithm is not straightforward. The critical rule is (PM12), because it is not obvious where the value to be matched should be split. It is worth to remark that expanding $S^*$ into $S, S^* + ()$, thus relying on the first policy for the choice schema to yield the longest matching prefix, does not always produce the desired results, as noted in [34]. Indeed, consider the schema $(a[ ] + a[ ], b[ ])^*, (b[ ] + O)$. This would be expanded into $((a[ ] + a[ ], b[ ]), (a[ ] + a[ ], b[ ])^* + O), (b[ ] + O)$ and the value $a[ ], b[ ]$ would be split into $a[ ]$ matching with $(a[ ] + a[ ], b[ ])^*$ and $b[ ]$ matching with $(b[ ] + O)$. However, $a[ ], b[ ]$ is the longest prefix matching with $(a[ ] + a[ ], b[ ])^*$ with $O$ matching with $(b[ ] + O)$. In order to implement the matching of a value $V$ against a pattern list $S^* \colon \Phi$, a naive implementation may attempt splitting the value beginning from its right end, trying first to match $(O)$ with $\Phi$ and $V$ with $S^*$. If this fails, the smallest non-void suffix of $V$ is matched against $\Phi$, and the remaining prefix against $S^*$, and so forth. More efficient solutions are discussed in the literature [17].

### 5.2 The (local) transition relation

Let $1, 1', \ldots$ range over a countably infinite set of locations. We assume a relation $@$ mapping channels to locations and we write $u@l$ for $u$ located at $l$. With an abuse of notation, we extend $-@l$ to variables. The relation $x@l$ is always true (since variables may be instantiated by channels located at $1$). The following transition relation is defined when subjects of selects and replications
Table 4
Local transition relation.

(tr1) \[
E \upharpoonright_{\text{dom}(\Gamma)} V \\
\Gamma \vdash u!(E) \quad \frac{1}{V} P_0
\]

(tr2) \[
\Gamma \vdash \{u_i@l_i\}_{i \in I} \\
\Gamma \vdash \text{select} \{u_i?(F_i)P_i \quad i \in I\} \quad \frac{u_i?!((F_i))}{P_i}
\]

(tr3) \[
\Gamma \vdash u: \langle S \rangle^\kappa \quad \frac{P \rightarrow u \in \overline{\text{fv}(\mu)} \cup \overline{\text{bv}(\mu)}}{\Gamma \vdash \text{new} u: \langle S \rangle^\kappa \quad \text{in} P \rightarrow ^\mu \text{new} u: \langle S \rangle^\kappa \quad \text{in} Q}
\]

(tr4) \[
\Gamma \vdash v: \langle S \rangle^\kappa \quad \frac{P \rightarrow u \in \overline{\text{fv}(\mu)} \cup \overline{\text{bv}(\mu)}}{\Gamma \vdash \text{new} v: \langle S \rangle^\kappa \quad \text{in} P \rightarrow ^{\langle \Gamma' + v: \langle S \rangle^\kappa \rangle u}(V)} Q
\]

(tr5) \[
\Gamma \vdash u \in \langle S \rangle^\kappa \quad \frac{P \rightarrow \text{match } E \text{ with } \{ F_i \Rightarrow P_i \quad i \in \gamma \}}{\Gamma \vdash P \rightarrow \text{spawn } \{ F_i \} \rightarrow P_\gamma}
\]

(tr6) \[
\Gamma \vdash (\Gamma' u)!(V) \quad \frac{P' \rightarrow \text{spawn } \{ Q \} \rightarrow \text{spawn } \{ P' \} \rightarrow Q}{\Gamma \vdash \text{spawn } \{ P \} \rightarrow \text{spawn } \{ Q \} \rightarrow \text{spawn } \{ P' \} \rightarrow Q'}
\]

(tr7) \[
\Gamma \vdash P \rightarrow P' \quad \frac{\text{bv}(\mu) \cap \text{fv}(Q) = \emptyset}{\Gamma \vdash \text{spawn } \{ Q \} \rightarrow \text{spawn } \{ P' \} \rightarrow Q'}
\]

(tr8) \[
\Gamma \vdash (\Gamma' u)!(V) \quad \frac{P' \rightarrow \text{spawn } \{ Q \} \rightarrow \text{spawn } \{ P' \} \rightarrow Q'}{\Gamma \vdash \text{spawn } \{ P \} \rightarrow \text{spawn } \{ Q \} \rightarrow \text{spawn } \{ P' \} \rightarrow Q'}
\]

(u@l) \[
\Gamma \vdash u* (F) \quad \frac{u?!((F))}{\text{spawn } \{ P \} \rightarrow \text{spawn } \{ P' \} \rightarrow Q'}
\]

are local to the PiDuce runtime environment. The general case is discussed in
Section 6.

Let \( \mu \) range over input labels \( u?((F)) \), bound output labels \( \Gamma u!((V)) \) with
\( \text{dom}(\Gamma) \subseteq \text{fv}(V) \), and \( \tau \). Let also \( \text{fv}(u?((F))) = \{ u \} \), \( \text{fv}(\Gamma u!((V))) = \{ u \} \cup \langle \text{fv}(V) \setminus \text{dom}(\Gamma) \rangle \), \( \text{bv}(u?((F))) = \text{fv}(F) \), \( \text{bv}(\Gamma u!((V))) = \text{dom}(\Gamma) \), and \( \text{fv}(\tau) = \text{bv}(\tau) = \emptyset \). The (local) transition relation of PiDuce, \( \Gamma \vdash P \rightarrow Q \), is the
least relation satisfying the rules in Table 4 plus the symmetric of the com-
munication rule (tr8).

The transition relation is also closed under alpha-conversion. For example, if
\( \Gamma \vdash P \rightarrow (\Gamma' u)!(V) \alpha \) then \( \Gamma \vdash P \rightarrow (\Gamma' \alpha u)!((V) \alpha) \alpha \) for every alpha-conversion \( \alpha \).

The transition relation of Table 4 is similar to that of the pi calculus [29],
except for the environment \( \Gamma \), which is partially supplied by enclosing \textbf{new}
operators and partially by the global environment.

We discuss rules (tr1), (tr3), (tr4), (tr5), and (tr8); the arguments about
the other rules are omitted. Rule (TR1) defines the semantics of \( u! (E) \). According to this semantics, \( E \) is evaluated into a \( \text{dom}(\Gamma) \)-value \( V \) and \( V \) is delivered. Rules (TR3) and (TR4) define the semantics of outputs when they are underneath local definitions of channels. There are two cases: (i) the local channel does not occur in the message, (ii) the local channel does occur. The case (i) is managed by (TR3): in this case the output operation is simply lifted outside the \texttt{new} and the label of the transition does not change. The case (ii) is managed by (TR4). The label gathers the local channels (and their schema) that are transmitted. The third hypothesis of (TR4) verifies that the channel \( v \) occurs in the message; in this case the environment of the label in the conclusion is extended with \( v \) and its schema. This extension of the label, which is different from pi calculus for the presence of schemas, is meant to capture the property that when a Web service \texttt{URL} is shipped, the \texttt{WSDL} document is also sent. (This \texttt{WSDL} contains, for instance, the protocol that must be used to invoke the service and the schemas of arguments and of the result.) Rule (TR5) defines the semantics of \( \text{match } E \text{ with } \{ F_i \Rightarrow P_i ; i \in 1..n \} \). According to this rule, \( E \) is evaluated, then the first pattern \( F_j \) matching the value is chosen and the continuation \( P_j \) is run with the substitution returned by the pattern matching algorithm. Rule (TR8) makes two parallel processes emitting and receiving a message on the same channel communicate. To this aim the message is matched against the pattern and the resulting substitution is applied to the receiver process. It is worth to notice that our semantics admits communications on variables that are channels. This case intends to model those communications involving channels that have not been published (the \texttt{WSDL} has not been created) as their declaration has been lifted to the label of the transition relation, but they do not occur in the domain of the environment. The publication happens as soon as the channel is extruded to a remote machine (see rule (DTR1) in Section 6).\(^1\)

### 6 Distributed operational semantics

The underlying model of \texttt{PiDuce} is distributed; it consists of a number of runtime environments – that may be \texttt{PiDuce} runtimes or not –, which execute at different locations and interact by exchanging messages over channels. In this section we describe the distributed semantics of the \texttt{PiDuce} language.

A \texttt{PiDuce} machine is a collection of runtime environments:

\[
\Gamma_1 \vdash_{1} P_1 \parallel \cdots \parallel \Gamma_n \vdash_{1} P_n
\]

such that

\(^1\) The \texttt{PiDuce} implementation eagerly creates the \texttt{WSDL} interface of a service as soon as the corresponding \texttt{new} in the object code is executed.
(1) \( l_1, \ldots, l_n \) are pairwise different;
(2) \( \Gamma_1, \ldots, \Gamma_n \) are localized with respect to \( l_1, \ldots, l_n \), namely \( u \in \text{dom}(\Gamma_i) \)
and \( u@l_j \) implies \( u \in \text{dom}(\Gamma_j) \).

PiDuce machines are ranged over by \( M, N \), etc. We also let \( \text{dom}(\Gamma_1 \vdash l_1 \parallel \cdots \parallel \Gamma_n \vdash l_n) = \bigcup_{i \in 1\ldots n} \text{dom}(\Gamma_i) \). Processes in the runtime environments extend those of Table 1 with operations dealing with remote locations:

- **input on remotely located channels**: the subjects \( u_i \) in \( \text{select} \{ u_i?((F_i)P_i) \}_{i \in I} \) may be non-local;
- **new at remote location**: the process \( \text{new } u : \langle S \rangle^0 \text{ at } l \text{ in } P \) delegates the runtime environment located at \( l \), which may be remote, to create the runtime support for \( u \). The syntax requires the capability of the schema to be \( \text{IO} \) because in order for the operation to be useful the continuation \( P \) needs to be able to perform both input and output operations on \( u \);
- **import of services**: the process \( \text{import } u : S \rightarrow T = v \text{ in } P \) downloads the WSDL of the channel \( v \), verifies that it is a subschema of \( \langle S, (T)^0 \rangle^0 \) and replaces \( u \) with \( v \) in the continuation \( P \). The channel \( v \) represents a synchronous – request-response in WSDL jargon – operation in a remote service. A special case of this process is \( \text{import } u : \langle S \rangle^0 = v \text{ in } P \) that verifies the WSDL of \( v \) to be a subschema of \( \langle S \rangle^0 \). In this section the notation \( S \rightarrow T \) may be considered as syntactic sugar for the schema \( \langle S, (T)^0 \rangle^0 \); the differences between \( S \rightarrow T \) and \( \langle S, (T)^0 \rangle^0 \) have to do with interoperability and will be discussed in Section 7.1.

Among these operators, **import** is the most interesting one because it permits PiDuce processes to access existing services. For example, the code

```
import fact : Int → Int = "www.mathfunctions.edu/fact"
in new u : \langle int \rangle^0
in spawn \{ fact!(5,u) \} u?(v:Int) printInt!(v)
```

imports the operation \( \text{fact} \) which is provided by a Web service located at \url{www.mathfunctions.edu/fact}, invokes \( \text{fact} \) with 5, and prints the result.

The runtime environment also uses a further operation dealing with remote locations:

- **linear forwarder** \( u \rightarrow v \) that forwards a message on a channel \( u \) to \( v \). This operator implements input operations on remotely located channels; its theory has been developed in [18] and will be recalled below.

The type system of Table 2 is extended with the rules in Table 5 for \text{new} binders at remote locations, imports and linear forwarders. Rule \text{(NEWAT)} types the creation of channels at remote locations; the typing rule is similar to \text{(NEW)}. Rules \text{(IMPORT)} and \text{(IMPORT-A)} type import of channels by checking \( P \) to
Table 5

Typing rules for distributed PiDuce.

\[
\begin{align*}
\text{\texttt{(newat)}} & \quad (\Gamma; \Delta) + u : \langle S \rangle^{10} \vdash P \\
\Gamma; \Delta \vdash \text{new} \ u : \langle S \rangle^{10} \text{ at } l \text{ in } P & \quad \Rightarrow \\
\text{\texttt{(import)}} & \quad (\Gamma; \Delta) + u : \langle S, (T)^{0} \rangle^{0} \vdash P \\
\Gamma; \Delta \vdash \text{import} \ u : S \rightarrow T = v \text{ in } P & \quad \Rightarrow \\
\text{\texttt{(import-\lambda)}} & \quad (\Gamma; \Delta) + u : \langle S \rangle^{0} \vdash P \\
\Gamma; \Delta \vdash \text{import} \ u : \langle S \rangle^{0} = v \text{ in } P & \quad \Rightarrow \\
\text{\texttt{(lforwd)}} & \quad \Gamma \vdash \text{v} : \langle S \rangle^{0} \\
\Gamma; \Delta \vdash \text{u} \Rightarrow \text{v} & \quad \Rightarrow \\
\end{align*}
\]

be well-typed in \((\Gamma; \Delta) + u : R\) (\(u\) is removed from \(\Delta\) because it is not a local channel), where \(R\) is \(\langle S, (T)^{0} \rangle^{0}\) or \(\langle S \rangle^{0}\), according to whether \(v\) is a request-response operation or not. The rules also verify that the schema of the imported channel, which is stored in the global environment, is compatible with \(R\). Rule \((\text{lforwd})\) types linear forwarders. The hypotheses, which require that \(u\) and \(v\) can be used for respectively receiving and sending values, are in correspondence with those for typing the process \(\text{select} \ \{ u? (x : R) \ v!(x) \} \) – where \(R\) is the schema of the messages accepted by \(u\) – with the following additional constraints:

1. the schema of \(u\) is taken from the global environment because \(u\) is not local;
2. the schema of \(v\) is taken from the global environment as well, because the linear forwarder process is executed on a remote machine;
3. no subschema of \(\Gamma(v)\) is considered because processes \(u \Rightarrow v\) are generated by the PiDuce runtime and, by definition, \(v\) always has a schema of shape \(\langle S \rangle^{0}\).

Typing is extended to machines as follows. Let \([\Gamma]^{10}_{\text{I}}\) be the environment

\[
[\Gamma]^{10}_{\text{I}}(u) = \begin{cases} 
\langle S \rangle^{10} & \text{if } u \Rightarrow 1 \text{ and } \Gamma(u) = \langle S \rangle^{\kappa} \\
\text{undefined} & \text{otherwise}
\end{cases}
\]

The operation \([\Gamma]^{10}_{\text{I}}\) is meant to define the environment for local channels: it extracts the channels local at 1 out of \(\Gamma\) and replaces the capability with 10 because 10 is the capability of local channels (cf. rule \((\text{new})\) in Table 2). We recall that, according to our notation, if \(x\) is a variable in \(\text{dom}(\Gamma)\) and \(\Gamma(x)\) is a channel schema, then \(x \in \text{dom}([\Gamma]^{10}_{\text{I}})\), too, because \(x \Rightarrow 1\) is always true.

Let \(\vdash M\), read \(M\) is \textit{well-typed}, if the following properties hold:

(i) for every \(\Gamma \vdash P\) in \(M\): \(\Gamma; [\Gamma]^{10}_{\text{I}} \vdash P\) and
(ii) (\textit{machine consistency}) if \(\Gamma \vdash P\) and \(\Gamma' \vdash P'\) in \(M\) and \(u \in \text{dom}(\Gamma')\) and \(u \Rightarrow 1\), then \(u \in \text{dom}(\Gamma)\) and \(\Gamma(u) \triangleleft \Gamma'(u)\). (This constraint only
regards variables with channel schemas.)

Therefore, a machine is well-typed if every runtime environment in it is well-typed and the runtime environments access to remote channels with schemas that are superschemas of the actual ones. This is also the case for global accesses that are located at the same runtime environment (take $l = l'$ in case (iii)). For instance, when $v$ is located at the same runtime environment executing **import** $u: \langle S \rangle^0 \equiv v$ in $P$. We notice that if $\vdash M \parallel N$ then $\vdash M$ and $\vdash N$.

Next we extend the (local) transition relation with the semantics of the operations dealing with remote locations. To this aim we drop the assumption in Section 5 that subjects of selects are local to the PiDuce runtime environment, as well as that new channels are always created locally to the runtime environment. In order to account for the new operations we extend the notation so that $\mu$ also ranges over the labels $u: S$, ($u@l : S$), and $(\Gamma)u \rightarrow v$ with $\text{dom}(\Gamma) \subseteq \{v\}$, too. Let $fv(\langle u@l : S \rangle) = \{u\}$, $fv((u : S)) = \emptyset$, $fv((\Gamma)u \rightarrow v) = \{u, v\} \setminus \text{dom}(\Gamma)$ and let $bv((u : S)) = \emptyset$, $bv((\langle u@l : S \rangle)) = \{u\}$, $bv((\Gamma)u \rightarrow v) = \text{dom}(\Gamma)$. We write $\text{spawn}_{i \in 1..n} \{P_i\} \cdot Q$ for $\text{spawn} \{P_1\} \ldots \text{spawn} \{P_n\} \cdot Q$. As usual $\uplus$ denotes disjoint union. The transition relations use the following operations on environments:

$\Gamma@1$ restricts $\Gamma$ to variables located at $1$:

$$
(\Gamma@1)(u) = \begin{cases} 
\Gamma(u) & \text{if } u \in \text{dom}(\Gamma) \text{ and } u@1 \\
\text{undefined} & \text{otherwise}
\end{cases}
$$

$\Gamma \setminus 1$ removes from $\Gamma$ the variables located at $1$:

$$
(\Gamma \setminus 1)(u) = \begin{cases} 
\Gamma(u) & \text{if } u \in \text{dom}(\Gamma) \text{ and not } (u@1) \\
\text{undefined} & \text{otherwise}
\end{cases}
$$

We write $\Gamma \setminus 1,1'$ for $(\Gamma \setminus 1) \setminus 1'$.

$\Gamma \text{ meet } \Gamma'$ defines an environment that includes the domains of $\Gamma$ and $\Gamma'$ and that associates to every variable a subschema of those associated by $\Gamma$ and $\Gamma'$:

$$
(\Gamma \text{ meet } \Gamma')(u) = \begin{cases} 
\Gamma(u) & \text{if } u \in \text{dom}(\Gamma) \setminus \text{dom}(\Gamma') \\
\Gamma'(u) & \text{if } u \in \text{dom}(\Gamma') \setminus \text{dom}(\Gamma) \\
S & \text{if } u \in \text{dom}(\Gamma) \cap \text{dom}(\Gamma') \\
\text{and } S <: \Gamma(u) \text{ and } S <: \Gamma'(u) \\
\text{undefined} & \text{otherwise}
\end{cases}
$$

The **meet** operation is used in the transition relation to guess the schema of channels in messages that are located at neither the source nor the destination runtime environment.
12

Table 6
Distributed transition relation.

Table 6
Distributed transition relation.

The transition relation $\Gamma \vdash_1 P \xrightarrow{\tau} Q$ and the distributed transition relation $\mathcal{M} \xrightarrow{\Delta} \mathcal{N}$ of PiDuce are the least relations satisfying the rules in Section 5 plus those in Table 6 (for the sake of brevity we omit $\Delta$ when it is the empty context). The distributed transition relation is closed under commutativity and associativity of $\parallel$. The label $\Delta$ on the distributed transition relation represents a set of assumptions regarding the type of free channels that two machines have exchanged between each other, where none of the machines hosts the exchanged channels.
Rule (TR10) defines selects with remote subjects. It translates the select process on-the-fly into another one using a local select. (This translation has been proposed for encoding distributed choice in [18].) To explain the transition we discuss the case of a select with three branches, one with a local subject \(u\) and the others with remote subjects \(v\) and \(w\):

\[
\text{select } \{u?(F)P \quad v?(F')Q \quad w?(F'')R\}
\]

This select may be turned into a local one by creating two (local) siblings for \(v\) and \(w\), let them be \(v'\) and \(w'\), respectively, and communicating to the channel managers of \(v\) and \(w\) the presence of these siblings. So the above process may be translated into

\[
\text{new } v', w' : S', T' \text{ in } \text{spawn } \{v \rightarrow v'\} \text{ spawn } \{w \rightarrow w'\} \\
\text{select } \{u?(F)P \quad v'?(F')Q \quad w'?(F'')R\}
\]

However this translation is too rough because of the following problem. The purpose of the linear forwarder \(v \rightarrow v'\) is to migrate to the remote location of \(v\) and forward one message to the location of \(v'\). Similarly for \(w \rightarrow w'\). By rule (TR2), the branch \(u?(F)P\) may be chosen because of the presence of a message on \(u\). This choice destroys the branches \(v'?(F')Q\) and \(w'?(F'')R\). Therefore, when messages for \(v'\) and \(w'\) will be delivered by the remote machines, such messages will never be consumed. To avoid these misbehaviors, one has to compensate the previous emission of linear forwarders by undoing them with \(v'?(x : S') v!(x)\) and \(w'?(x : T') w!(x)\). In case the picked branch is \(v'?(F')Q\), by a similar argument, we have to compensate only one linear forwarder – the \(w \rightarrow w'\). Therefore the correct translation for the distributed select is:

\[
\text{new } v', w' : S', T' \text{ in } \text{spawn } \{v \rightarrow v'\} \text{ spawn } \{w \rightarrow w'\} \\
\text{select } \{u?(F)(\text{spawn } \{v'?(x : S') v!(x)\}) \\
\quad \text{spawn } \{w'?(x : T') v!(x)\} \quad P) \\
\quad v'?(F')(\text{spawn } \{w'?(x : T') v!(x)\} \quad Q) \\
\quad w'?(F'')(\text{spawn } \{v'?(x : S') v!(x)\} \quad R) \}
\]

that is the term yielded by the (TR10) in this case. Rule (TR11) creates a channel remotely located at \(1'\). To this aim a channel located at \(1'\) is taken and the local name is replaced by this channel in the continuation. When \(1 = 1'\), the process \text{new } u : \langle S \rangle^10 \text{ in } P\) is simply an abbreviation for \text{new } u : \langle S \rangle^10 \text{ at } 1' \text{ in } P\). In this case its semantics is defined by rules (TR3) and (TR4). Rule (DTR2) guarantees that such a channel is fresh at the remote location. Rule (TR12) imports a channel (the compiler type-checks the continuation under the assumption \(u : S \) – see (IMPORT)). Rule (TR13) lifts the linear forwarder to the label. This rule and rule (DTR3) define a linear forwarder \(u \rightarrow v\) as a small atom migrating to the remote location of \(u\) and becoming the process \(u?(x : S) v!(x)\). Rule (TR14) accounts for linear for-
warders $u \rightarrow v$ where $v$ is local to the sender. In this case the environment of the receiver must be extended adequately.

Rule (dtr1) models the delivery of a message to a remote runtime environment $1'$. When this occurs all the bound channels are created in the sender location $1$ and the message is put in parallel with every process running at $1'$. The rule extends the environments of $1$ and $1'$ with the new channels $v_i \in I$. Additionally, the environment $\Gamma'$ of $1'$ is extended with channels in $\mathbf{fv}(V) \setminus \{v_i \in I\}$ that are either undefined in $\Gamma'$ or whose associated schema is too large. This is a subtle problem to deal with. Consider a channel $v \in \mathbf{fv}(V) \setminus \{v_i \in I\}$ that is located at $1$. The machine at $1'$ may already be aware of such channel either because it has been imported or because it has been received during a previous communication. The point is that $\Gamma(v)$ and $\Gamma'(v)$ are not equal in general. In particular, by the definition of $\vdash M, \Gamma(v) \not\vdash \Gamma'(v)$. Therefore the rule (dtr1) updates the environment of $1'$ with $(\Gamma|_{\mathbf{fv}(V)})_1$. A similar problem is manifested by channels $v \in \mathbf{fv}(V) \setminus \{v_i \in I\}$ that are not located at $1$ nor at $1'$. In this case $\Gamma(v)$ and $\Gamma'(v)$ may be incomparable, as in general they are superschemas of the actual schema of $v$, which is defined on a machine $1''$ other than $1$ and $1'$. Therefore we guess the right schema – the operation $\text{meet}$ – and publish our guess in the label of the transition. It is the rule (dtr5) that checks the correctness of our guess when the right context environment is found. The rule removes the checked bindings from the environment, that is a successful distributed transition of a PiDuce machine has always labels with empty environments.  

The other rules have been already described, except (dtr4) that lifts transitions in components to composite machines.

We conclude this section by asserting the soundness of the static semantics. Proofs are reported in the Appendix B. The first property, subject reduction, states that well-typed processes always transit to well-typed processes.

**Theorem 6 (Subject Reduction)** Let $\Gamma; [\Gamma]^{10}_1 \vdash P$. Then

1. If $\Gamma \vdash P \xrightarrow{(\Gamma')u \rightarrow v (V)} Q$, then (a) $\Gamma + \Gamma'$; $[\Gamma + \Gamma']^{10}_2 \vdash Q$, (b) $\Gamma + [\Gamma]^{10}_2 \vdash u : S$, $\Gamma + \Gamma' \vdash V : T$ and $S < : (T)^0$;
2. If $\Gamma \vdash P \xrightarrow{u ?(F)} Q$, then (a) $\Gamma; [\Gamma]^{10}_2 + \mathbf{Env}(F) \vdash Q$ and (b) $\Gamma + [\Gamma]^{10}_2 \vdash u : S$ with $S < : (\text{schof}(F))^2$;
3. If $\Gamma \vdash P \xrightarrow{(\Gamma')u \rightarrow v} Q$, then (a) $\Gamma + \Gamma'$; $[\Gamma + \Gamma']^{10}_2 \vdash Q$ and (b) $\Gamma \vdash u : S$, $\Gamma + \Gamma' \vdash v : (T)^0$ and $S < : (T)^1$;
4. If $\Gamma \vdash P \xrightarrow{(u \rightarrow (S))^{10}} Q$, then $\Gamma; [\Gamma]^{10}_2 + u : (S)^0 \vdash Q$;
5. If $\Gamma \vdash P \xrightarrow{\tau} Q$, then $\Gamma; [\Gamma]^{10}_2 \vdash Q$.

2 In the implementation this problem does not arise and there is no need for the $\text{meet}$ operation as there is only one global environment that is shared among all the runtime environments.
Let $\vdash M$. Then

(6) if $M \xrightarrow{\Delta} N$, then $\vdash N$.

The first item of the subject reduction entails that the reduct $Q$ of a $(\Gamma')u!(V)$-transition is typable provided the initial process $P$ is typable. To this aim, the environment $\Gamma'$; $[\Gamma']_1^{\lozenge}$ must be suitably extended with the bindings in $\Gamma'$. This extension is similar to the one used in the rule (NEW) of the type system. In facts, bindings in $\Gamma'$ are collected by surrounding new binders – see rule (TR4).

The second item deals with inputs and entails the typability of the reduct in an environment extended with that of patterns. The subject reduction guarantees the exhaustivity of inputs. The third item is about linear forwarders. Such operations are introduced by PiDuce runtimes as described by rule (TR10). Therefore $v$ must have schema $\langle T \rangle^\sigma$, for some $T$; the theorem guarantees that $u$ has a schema $S$ “compatible” with $\langle T \rangle^\sigma$, namely $S \subset: \langle T \rangle^\gamma$. The fourth item deals with creation of remote channels. The other items are not commented because obvious.

The second soundness property concerns progress, that is, an output on a channel will be consumed if an input on the same channel is available and a message or a linear forwarder is delivered to the remote runtime when it is present (we are assuming the absence of failures). In order to guarantee progress, it is necessary to restrict (well-formed) environments. To illustrate the problem, consider the following judgment:

\[
\begin{align*}
  u: (\text{int }+ \text{ string})^\kappa, v: \text{int }+ \text{ string} & \vdash_1 \text{spawn } \{u!(v)\} \ u?(x: \text{int }+ \text{ string}) \\
  & \quad \text{match } x \text{ with } \{\text{int } \Rightarrow P \quad \text{string } \Rightarrow Q\} 
\end{align*}
\]

The reader may verify that this judgment can be derived in our type system. However, after the communication, the pattern matching fails because the schema of $v$ is neither a subschema of int nor of string (see rule (PM5)). Another example is the following. Let $\Gamma$ be $u: a[b[ ]], V = u$, and $F = a[v: b[ ]]$. Then $\Gamma \vdash V: S$ and $S \subset: \text{schof}(F)$ but there is no $\sigma$ such that $\Gamma \vdash V \in F \leadsto \sigma$. In fact these circumstances never occur in practice: if a value is sent, it may contain either labels or constants or channels. Under this constraint, progress is always guaranteed.

We say that $\Gamma$ is channeled if, for every $u \in \text{dom}(\Gamma)$, $\Gamma(u)$ is a channel schema.

**Theorem 7 (Progress)** Let $\Gamma$ be channeled.

1. If $\Gamma \vdash V: S$ and $S \subset: \text{schof}(F)$, then there is $\sigma$ such that $\Gamma \vdash V \in F \leadsto \sigma$;
2. If $\Gamma; [\Gamma]_1^{\lozenge} \vdash P$, $\Gamma \vdash_1 P \xrightarrow{(\Gamma')_{u!(V)}} Q'$, and $\Gamma \vdash_1 P \xrightarrow{u?(F)} Q''$, then there is $Q$ such that $\Gamma \vdash_1 P \xrightarrow{\sigma} Q$;
3. If $\vdash (\Gamma \vdash_1 P \parallel M)$, $\Gamma \vdash_1 P \xrightarrow{(\Gamma')_{u!(V)}} Q$, and $u$ is located at a location of
\[ M, \; \text{then} \; \Gamma \vdash_1 P \parallel M \xrightarrow{\Delta} \Gamma \vdash_1 Q \parallel N, \; \text{for some} \; N. \]  
Similarly when the label is \((\Gamma')u \rightarrow v\).

7 PiDuce and Web services

The language presented in the previous sections deals with all the fundamental aspects of Web service definitions and interactions. However, there is still a gap between PiDuce and the current technologies related to Web services. Such gap is finally closed in this section by extending PiDuce with additional constructs, though the primitive operations of the calculus are unchanged in their essence.

7.1 Defining request-response services

The basic communication mechanism in PiDuce is the asynchronous message passing. Other mechanisms that are primitive in Web services, such as rendezvous, must be programmed by means of explicit continuations. In Section 6 we have already discussed the semantics of a construct that permits to import request-response operations. In that case, a request-response operation is typed with a schema \(\langle S, \langle T \rangle^0 \rangle^0\) and has the following intended behavior. When invoked, a fresh channel is sent with the actual data of type \(S\). At the same time, the invoker spawns an input process catching the response on the fresh channel. This behavior is actually a well-known encoding of rendez-vous, which is incongruous with respect to reality where request-response operations return results using the same connection. This is the reason why an explicit schema constructor \(S \rightarrow T\) has been used rather than \(\langle S, \langle T \rangle^0 \rangle^0\). The PiDuce runtime (in particular, the Web interface, see Section 8.1) implements the invocations of a channel with schema \(S \rightarrow T\) by extracting the actual data and continuation channel from the sent message, establishing a connection and sending the actual data over the connection, receiving the response from the same connection, and forwarding it on the continuation channel.

We can adopt a similar mechanism to define a service implementing a request-response operation. PiDuce processes are extended with

\[ \text{new } u:S \rightarrow T \text{ in } P \]

which differs from the \text{new} of Table 1 because the associated WSDL has its interaction pattern set to request-response, an input message part set to \(S\), and an output message part set \(T\). The behavior of \(u\) is the same as for the corresponding import.
7.2 Channels versus services

So far a one-to-one correspondence between PiDuce channels and Web services (hence between PiDuce channels and WSDL resources) has been assumed. This assumption falls short in faithfully modeling real Web services where a WSDL resource corresponds to a set of operations. To overcome this limitation we need to extend schemas and processes in Table 1. The extension, illustrated in Table 7, is folklore in the community except for the definition of the subschema relation.

Table 7
PiDuce syntax with service extensions (I is finite).

\[ S ::= \]
\[ \ldots \]
\[ \{ m_i : S_i \} \]
\[ \text{schema} \]
\[ \text{as in Table 1} \]
\[ \text{(record schema)} \]

\[ E ::= \]
\[ \ldots \]
\[ r \# m \]
\[ \text{expression} \]
\[ \text{as in Table 1} \]
\[ \text{(service operation)} \]

\[ P ::= \]
\[ \ldots \]
\[ \text{new } r : S \text{ in } P \]
\[ \text{import } r : S = v \text{ in } P \]
\[ \text{process} \]
\[ \text{as in Table 1} \]
\[ \text{(new)} \]
\[ \text{(import)} \]

The extended syntax uses the countably infinite sets of operation names, ranged over by \( m, n, \ldots \). Among variables we distinguish services ranged over by \( r, s, \ldots \). In the new syntax, \( u \) and \( v \) range over channels and expressions \( r \# m \).

The schema \( \{ m_i : S_i \} \), with \( I \) finite, describes services that offer a set of operations \( m_i \) whose schema is \( S_i \). Operation names in records are pairwise different; the schemas \( S_i \) are always channel schemas of shape \( \langle S \rangle^k \) or \( S \rightarrow T \). The definition of handle and the subschema relation of Definition 1 are extended with a further entry dealing with record schemas. Let \( \{ m_i : S_i \} \downarrow \{ m_i : S_i \} \), (). A subschema \( \mathcal{R} \) is a relation such that \( S \mathcal{R} T \) implies the items listed in Definition 1 and, in addition:

(5) \( S \downarrow \{ m_i : S_i \}, S' \) implies \( T \downarrow \{ m_j : T_j \}, T'_k \), for \( 1 \leq k \leq n \), with \( J_k \subseteq I \) and, for every \( j \in J_k \), \( S_j \mathcal{R} T_j \) and \( S' \mathcal{R} \sum_{k=1}^{n} T'_k \).

For example \( \{ m : \langle \text{int} \rangle^0 ; n : \langle \text{int} + \text{string} \rangle^0 \} \prec \{ n : \langle \text{int} \rangle^0 \} \) and \( \{ m : \langle \text{int} \rangle^0 ; n : \langle \text{string} \rangle^0 \}, \langle \text{int} + \text{string} \rangle \prec \{ m : \langle \text{int} \rangle^0 \}, \langle \text{int} \rangle \prec \{ n : \langle \text{string} \rangle^0 \}, \langle \text{string} \rangle \).

The process \textbf{new } r : \{ m_i : S_i \} \text{ in } P \text{ creates a service } r \text{ exposing the operations } m_i, i \in I \text{. The continuation } P \text{ addresses such operations with } r \# m_i \text{. In particular, since now } u \text{ and } v \text{ also range over expressions of the form } r \# m, \text{ outputs, selects, and replications may also have the shape } r \# m ! (E), \]
Table 8
Typing rules with service extensions.

Expressions:
\[ \Gamma \vdash r : \{ m_i : S_{i \in I} \} \quad k \in I \]
\[ \Gamma \vdash r \# m_k : S_k \]

Processes:
(NEW-s)
\[ \Gamma + r : \{ m_i : S_{i \in I} \} ; \Delta + r : \{ m_i : [S_{i}]_{10} \} \vdash P \]
\[ \Gamma ; \Delta \vdash \text{new } r : \{ m_i : S_{i \in I} \} \text{ in } P \]

(IMPORT-s)
\[ (\Gamma ; \Delta) + r : \{ m_i : S_{i \in I} \} \vdash P \]
\[ \Gamma(v) < : \{ m_i : S_{i \in I} \} \]
\[ \Gamma ; \Delta \vdash \text{import } r : \{ m_i : S_{i \in I} \} = v \text{ in } P \]

select \( \{ r_j \# m_j ?(F_j) \ P_j \}_{j \in J} \), and \( r \# m?*(F) \ P \), respectively. The relevant upshot for the implementation of PiDuce is that only one WSDL resource is published and associated with the service \( r \).

The process \( \text{import } r : \{ m_i : S_{i \in I} \} = v \text{ in } P \) imports the service whose WSDL interface is located at \( v \). This operation is successful provided that the schema of \( v \) contains at least the operations \( m_i \), and that the schema constraints are satisfied as described in Section 6.

The type system of Table 2 is also extended in order to cope with records. The extension is detailed in Table 8. The operation \( [S]_{10} \) is defined as follows:

\[ [S]_{10} = \begin{cases} 
\langle T \rangle_{10} & \text{if } S = \langle T \rangle^\alpha \\
\langle T, \langle R \rangle^0 \rangle_{10} & \text{if } S = T \rightarrow R
\end{cases} \]

The new rules (NEW-s) and (IMPORT-s) generalize (NEW) and (IMPORT) to references that are services. Theorem 6 and Theorem 7 still hold for this extension.

8 PiDuce architecture and interoperability

PiDuce runtime environments consist of three components: the virtual machine, the channel manager, and the Web interface – see Figure 3.

The virtual machine executes threads by interpreting PiDuce object code resulting from the compilation of PiDuce programs. The implementation of the
Fig. 3. **PiDuce**: the runtime environment.

The virtual machine is standard. The virtual machine stores its data in three structures: the *program pool*, containing the object code of the processes that have been loaded; the *ready queue*, containing threads that are ready to execute; the *blocked queue*, containing threads awaiting for some message. Threads are executed by means of a round-robin scheduler.

The *channel manager* handles the pool of channels that are local to the runtime environment. It is thus responsible for any operation involving local channels, in particular creation, send, and receive operations. Within the channel manager, each channel consists of a *schema*, describing the values that are carried, a *message queue* containing all the messages that have been sent but not consumed, and a *request queue* containing the threads waiting for a message on that channel. Whenever a new message arrives, the first thread in the request queue, if any, is awakened; otherwise the message is moved into the message queue.

The **PiDuce** runtime environment interacts with the external environment through a *Web interface*, which is responsible for bridging **PiDuce** processes and standard Web service technologies. In the outgoing direction, the Web interface is responsible for publishing appropriate **WSDL** resources for the **PiDuce** services created by the local virtual machine, for exporting **PiDuce** schemas into corresponding **XML**-Schemas, and for marshalling **PiDuce** values into **XML** messages. In the incoming direction, the Web interface is responsible for im-
porting WSDL resources as PiDuce services, for decoding XML-Schemas into PiDuce schemas, and for unmarshalling incoming XML messages into PiDuce values. Additionally, incoming XML messages are checked to be conformant to the schema of the channels they are targeted to, so as to prevent runtime errors within the virtual machine. The Web interface is also responsible for handling request-response channels and services as described in Section 7, so that within the virtual machine communication is purely asynchronous, whereas externally request-response services are handled in the standard way.

The modular design of this architecture has four main consequences: (1) the channel manager and the Web interface may be used stand-alone for providing PiDuce-compatible communication primitives in (native) programs that are written in a language other than PiDuce; (2) the virtual machine and the channel manager are decoupled from the actual transport protocols and technologies used in distributed communication. In this way a large part of PiDuce may be adapted to different contexts with minimum effort; (3) communications occurring within the same runtime environment are short-circuited and do not entail any additional overhead because they solely rely on internal data structures, rather than passing through the Web interface; (4) the virtual machine and the channel manager realize a type-safe environment: every operation performed therein can never manifest a type error.

8.1 Mechanisms interfacing PiDuce channels and Web services

Web services are published by interfaces that are written in a standard format: the WSDL – Web Service Description Language [25]. Every WSDL interface contains two parts: the abstract part defines the set of operations supported by the service; the concrete part binds every operation to a concrete network protocol and to a concrete location. Every operation is described by a name and by the schema of the messages that the operation accepts and/or produces. Albeit WSDL does not make any commitment on the schema language to be used, XML-Schema is the schema language universally adopted. Operations have an associated interaction pattern that conforms to one out of four models: one-way interaction (the client invokes a service by sending a message); notification (the service sends the message); request-response (the client sends a message and waits for the response); solicit-response (the service makes a request and waits for the response).

We discuss the possible WSDL interfaces by analyzing a number of examples. Consider the process new u:(S)* in P. This process creates a channel u and publishes it in a WSDL interface whose abstract part is:

```xml
<schema>
  <complexType name="InSchema">[S]</complexType>
</schema>
```
where $\lfloor S \rfloor$ is the XML-Schema encoding of the PiDuce schema $S$ (see Section 8.2.) This operation, being one-way, defines the "Input" message only and its schema "InSchema". It is worth to notice the use of the nonstandard attribute `piduce:operationCapability` which informs PiDuce clients that the service may support remote inputs if $\kappa \leq I$, as such information cannot be inferred from the WSDL interface. Since the attribute is in the `piduce` namespace, it will be ignored by standard Web services. The concrete part of the WSDL interface for $u$ is specified by two elements, `binding` and `service`:

```xml
1  <binding name="serviceSoap" type="service">
2    <soap:binding transport="http://schemas.xmlsoap.org/soap/http"/>
3    <operation name="operation">
4      <soap:operation style="document"
6        soapAction="http://www.cs.unibo.it:1811/x" />
7      <input><soap:body use="literal"></input>
8    </operation>
9  </binding>
```

The element `binding` defines the concrete message formats and the protocols to be used for accessing the operation. Currently, PiDuce supports the SOAP-over-HTTP binding – see line 2 of the above document. When using the SOAP-over-HTTP binding, the Web interface communicates SOAP messages (XML documents with the shape `Envelope[Header[headers], Body[parameters]]` where the `Header` is optional) using the HTTP protocol. The `soap:operation` element on line 4 has two attributes: `style` specifies that the operation style is `document` (the current prototype supports also the RPC style); `soapAction` specifies the SOAPAction header used in the HTTP request. The information in these two attributes, together with the attribute `use` of the `soap` element, specifies the format of the XML message to be sent. When the attribute `use` is literal then the transported XML message appears directly under the SOAP Body element without any additional encoding information. When the attribute `use` is encoded then the XML message is annotated with additional schema information. Therefore, a possible SOAP message for invoking a service having schema $\langle a[int] + b[string]\rangle$ is

```xml
<?xml version="1.0" encoding="utf-8"?>
```
The element `service` connects a binding to a specific URL. This URL is given by the location of the PiDuce runtime environment followed by a unique path, which is typically formed by appending the `?wsdl` suffix to the name of the channel. For instance, the following `service` element asserts that the service is located at `http://www.cs.unibo.it:1811/u`:

```xml
<service name="service">
  <port name="service" binding="serviceSoap">
    <soap:address location="http://www.cs.unibo.it:1811/u" />
  </port>
</service>
```

In addition to defining new channels, PiDuce also permits to import externally defined services. The process `import u:S = URL in P` imports a one-way interaction service located at `URL` and gives it the name `u`. When the bytecode corresponding to the import process is loaded into the virtual machine, the XML-Schema of the service `u` is extracted from the WSDL located at `URL`, it is decoded into a PiDuce schema `T`, and the decoded schema is verified to be compatible with `S` following rule (IMPORT-A). If the attribute `piduce:operationCapability="κ"` is found in the WSDL (implying that `u` has been published by a PiDuce runtime), compatibility means `S <: ⟨T⟩^κ`. Otherwise compatibility means `S <: ⟨T⟩^0`. The Web interface also verifies whether the binding is SOAP over HTTP. In case of success the value of the attribute `location` in the `service` element is used as target for future invocations. In case of failure of any of the above checks, the continuation `P` is not executed.

When the externally defined service is request-response, it may be imported by `import u:S \to T = URL in P`. The schema of `u` is retrieved as before but, in this case, the WSDL interface has a `portType` element whose shape is:

```xml
<portType name="op-request-response">
  <operation name="request-response">
    <input message="Input"/>
    <output message="Output"/>
  </operation>
</portType>
```

The Web interface decodes `Input` and `Output` into the schemas `S_I` and `S_O`, respectively. Then it verifies that `⟨S, ⟨T⟩^0⟩^0 <: ⟨S_I, ⟨S_O⟩^0⟩^0`. The remaining behavior is similar to the previous case.
8.2 From PiDuce schemas to XML-Schemas, and back

The correspondence between PiDuce schemas and XML-Schema is established by suitable encoding and decoding procedures implemented by the Web interface. By encoding we mean the translation of PiDuce schemas into XML-Schema, and by decoding we mean the inverse transformation.

Although PiDuce schemas and XML-Schema have a significant common intersection, there are features of XML-Schema not supported by PiDuce schemas and, conversely, features of PiDuce schemas that cannot be represented in XML-Schema. Regarding XML-Schema and the decoding function:

- XML attributes have been ignored because they would have entangled PiDuce schemas without giving any substantial contribution to their semantic relevance;
- features such as keys, references, and facets have been ignored because they are used mainly for validation (verifying that a value belongs to a given schema) rather than for typechecking (verifying that two schemas are related by the subschema relation).

In both cases such features are unused in the description of existing Web services (in particular in the XML-Schemas of the exchanged messages), hence omitting their treatment does not impede actual experimentation with PiDuce. For this subset of XML-Schema the decoding into PiDuce schemas is mostly straightforward. The only problematic case is for the all particle of XML-Schema that is used for defining sequences where elements can appear in any order. In this case the naive decoding into a PiDuce schema would result in a schema having an exponential size with respect to the number of elements occurring in the all particle. To alleviate this problem all is decoded as a single PiDuce sequence where elements are canonically ordered. When a value is received and validated by the Web interface against a PiDuce sequence originated by an all particle, the elements of the value are rearranged with the canonical order.

As regards the encoding function, PiDuce schemas that have a natural representation in XML-Schema are encoded by using standard elements in the XML-Schema namespace. The remaining PiDuce schemas are encoded using extension elements in a dedicated PiDuce namespace. In particular, extension elements are used for

- channel schemas, because current technologies do not provide any standard representation and description of them. We expect that this lack of expressiveness will be remedied in the near future, if higher-order Web services will prove to be a valuable feature;
- schema names, when these names are not the content of labelled values,
because such limitation of XML-Schema finds no justification in PiDuce schemas;

- unions and differences of labels, because these operations have been introduced in PiDuce mostly for pattern matching rather than for typing. In this case the lack of corresponding constructs in XML-Schema must not be interpreted as a weakness in XML-Schema itself. In fact, standard query and pattern languages such as XPath [13] and XQuery [8] provide for label wildcards.

It is understood that any WSDL interface containing schemas with extension elements will not be compatible with standard Web services.

9 Related work

The PiDuce prototype falls within the domain of distributed abstract machines for pi-like calculi. Among them we recall Facile [20], the Jocaml prototype [15], Distributed pi calculus [3], Nomadic Pict [32], the Ambient Calculus [10,30]. The differences between our model and the other ones are as follows. Facile uses two classes of distributed entities: (co-)located processes which execute, and channel-managers which mediate interaction. This forces it to use a handshake discipline for communication. Jocaml simplifies the model by combining input processes with channel-managers. However, it uses a quite different form of interaction, which does not relate that closely to pi calculus communication. It also forces a coarser granularity, in which every channel must be co-located with at least another one. Unlike Jocaml, our machine has finer granularity and uses the same form of interaction as the pi calculus. The other models add explicit location constructs to the pi calculus and use agent migrations for remote interactions.

PiDuce’s type system has been strongly influenced by the one in XDuce, a functional language for XML processing [21]. In XDuce, values do not carry channels, and the subschema relation is never needed at run-time. Our paper may also be read as an investigation of the extension of XDuce values and schemas with channels.

Several integrations of processes and semi-structured data have been studied in recent years. Two similar contributions, that are contemporary and independent to this one, are [12] and [2]. The schema language in [12] is the one of [6] enriched with the channel constructors for input, output, and input-output capability. No apparent restriction to reduce the computational complexity of pattern matching is proposed and no prototyping effort is undertaken. The schema language of [2] is simpler than that of PiDuce. In particular recursion is omitted and labeled schemas have singleton labels.
Other contributions integrating semi-structured data and processes are discussed in order. TulaFale [7], a process language with XML data, is especially designed to address Web services security issues such as vulnerability to XML rewriting attacks. The language has no static semantics. The integration of PiDuce with the security features of TulaFale seems a promising direction of research. Xdπ [19] is a language that supports dynamic Web page programming. This language is basically pi calculus with locations enriched with explicit primitives for process migration, for updating data, and for running a script. The emphasis of Xdπ is towards behavioral equivalences and analysis techniques for behavioral properties. A contribution similar to [19] is Active XML [1] that uses an underlying model consisting of a set of peer locations with data and services.

10 Conclusions

In this contribution we have presented the PiDuce project, a distributed implementation of the asynchronous pi calculus with tree-structured datatypes and pattern matching. The resulting language incorporates constructs that are suitable for modeling Web services, and this motivates our choice of XML idioms, such as XML-Schema and WSDL for types and interfaces, respectively. In this respect, PiDuce fills the gap between theory and practice by formally defining a programming language and showing its implementation using industrial standards.

Figure 4 shows a PiDuce client that interacts with the Web services provided by the on-line store Amazon and the Google search engine. The code shown is actually an approximation of the actual client, which needs a long preamble of complex schema definitions and slightly more complex messages to be sent to the two services; the full example can be found in the latest PiDuce distribution. The client starts by defining the relevant schemas that are published in the WSDL’s of the two Web services (lines 1 and 2). In fact, PiDuce provides an utility for extracting such declarations automatically, given the URL of the service’s WSDL file. Lines 3 to 9 import the two Web services. For each service we only import the relevant operations. In this case they are both request-response operations, as can be noticed by the arrow schema. The URL’s after the keyword location refer to the WSDL files provided by Amazon and Google. Line 10 defines a local channel to be used as the continuation for the interaction with the Amazon Web service. While PiDuce’s Web interface inter-operates natively with request-response operations, the language only provides for asynchronous communication primitives. Adding syntactic sugar for invoking synchronous operations is trivial. Line 11 defines a special channel used to write values on the terminal, so that the process can be monitored and the results can be printed. Lines 12 to 15 invoke Amazon by searching for a partic-
Fig. 4. A PiDuce client interacting with both Amazon and Google Web services.

Regarding the description of Web services interfaces, it is remarkable that WSDL 1.1 (already published as a W3C Note [25]) does not consider service references as first class values, that is natural in a distributed setting, in pi calculus, and, thereafter, in PiDuce. This lack of expressiveness has been at least partly amended in WSDL 2.0 [26,27] that, at the time of this writing, is in a Candidate Recommendation status. Still, we note significant differences between our approach and the way “Web services as values” are handled in WSDL 2.0. For example the client receiving a service reference u must eventually compare the schema in the WSDL of u with some local schema before using u or forwarding u to a third party. While this comparison, called subschema relation in this paper, is fundamental in PiDuce, it has been completely overlooked in WSDL 2.0.
Few remarks about XML-Schema are in order. First of all there is a large overlapping between XML-Schema and PiDuce schemas, which has been discussed in Section 8. Apart from channel schemas, the other major departure from XML schema is the support for nondeterministic labelled schemas. These schemas make the computational complexity of the subschema relation exponential, but they are essential for the static semantics of a basic operator in PiDuce, the pattern-matching (see the third premise of rule (match) in Table 2). Noticeably, the constraint of label-determinedness on channel schemas guarantees a polynomial cost for the subschema relation (and for the pattern matching) at runtime (see Appendix C).

Future work in the PiDuce project is planned in two directions: the first direction is rather pragmatic, and is aimed to improving interoperability and support to existing protocols. The goal is to interface PiDuce with more real-world Web services and to carry on more advance experimentation. The other direction regards conceptual features that are desirable and that cannot be expressed conveniently in the current model. In particular error handling and transactional mechanisms. These mechanisms, which are basic in BPEL [5], permit the coordination of processes located on different machines by means of time constraints. This is a well-known problematic issue in concurrency theory. An initial investigation about transactions in the setting of the asynchronous pi calculus has been undertaken in [23]. A core BPEL language without such advanced coordination mechanisms should be compilable in PiDuce without much effort, thus equipping BPEL with a powerful static semantics. We expect to define a translation in the near future.

Another direction of research is about dynamic XML data, namely those data containing active parts that may be executed on clients’ machines. This is obtained by transmitting processes during communications, a feature called process migration. The PiDuce prototype disallows program deployments on the network. However, the step towards migration is quite short due to the fact that object code is in XML format. Therefore it suffices to introduce two new schemas: the object code schema and the environment schema, and admit channels carrying messages of such schemas.

References


A Properties of the subschema relation

This appendix contains the proofs of Proposition 2. The statement is recalled for readability sake.

**Proposition 2**  
(1) \(<:\) is reflexive and transitive;  
(2) If \(S\) is empty, then \(S <: \text{Empty}\);  
(3) (Contravariance of \(\langle \cdot \rangle^0\)) \(S <: T\) if and only if \(\langle T \rangle^0 <: \langle S \rangle^0\);  
(4) (Covariance of \(\langle \cdot \rangle^I\)) \(S <: T\) if and only if \(\langle S \rangle^I <: \langle T \rangle^I\);  
(5) (Invariance of \(\langle \cdot \rangle^{10}\)) \(S <: T\) and \(T <: S\) if and only if \(\langle S \rangle^{10} <: \langle T \rangle^{10}\);  
(6) If \(S <: T\), then \(S,\emptyset <: T\); if \(\emptyset, S <: T\), then \(S <: T\);  
(7) If \(S <: T\) and \(S' <: T'\), then \(S,S' <: T,T'\);  
(8) If \((S + S'),S'' <: T\), then \(S,S'' <: T\) and \(S',S'' <: T\);  
(9) For every \(S\), \(\text{Empty} <: S <: \text{Any}\) and \(\langle S \rangle^\kappa <: \text{AnyChan}\) and \(\langle \text{Any} \rangle^{10} <: \langle S \rangle^0\) and \(\langle \text{Empty} \rangle^{10} <: \langle S \rangle^I\).

**Proof:** We prove items 1 (transitivity), 7, and 9.

As regards transitivity of item 1, let \(\mathcal{R}\) be a subschema relation and let \(\mathcal{R}^+\) be the least relation that contains \(\mathcal{R}\) and is closed under the following operations
(1) if $S \mathcal{R}^+ T$ then $S \mathcal{R}^+ T + R$;
(2) if $S \mathcal{R}^+ T$ and $S' \mathcal{R}^+ T$ then $S + S' \mathcal{R}^+ T$;
(3) if $S \mathcal{R}^+ T$ and $S \downarrow L[S'], S''$ then $L'[S'], S'' \mathcal{R}^+ T$ with $\widehat{L'} \subseteq \widehat{L}$.

It is easy to verify that $\mathcal{R}^+$ is a subschema relation. Let $\mathcal{R}$ and $\mathcal{S}$ be two subschema relations such that $\mathcal{S} \mathcal{R} T$ and $T \mathcal{S} R$. We prove that

$$T = \{(S, R) \mid S \mathcal{R}^+ T \text{ and } T \mathcal{S}^+ R\}$$

is a subschema relation. Let $S \mathcal{T} R$. The critical case is when $S \downarrow L[S'], S''$. According to the definition of $\mathcal{T}$, there exists $T$ such that $S \mathcal{R}^+ T$ and $T \mathcal{S}^+ R$. By Definition 1, $T \downarrow L'[T'], T''$ with $\widehat{L} \cap \widehat{L'} \neq \emptyset$. There are two cases:

(a) $T \downarrow L'[T'], T''$ with $\widehat{L} \subset L'$ and $\widehat{L} \cap \widehat{L'} \neq \emptyset$. We are reduced to $(L \cap L')[S'], S'' \mathcal{T} R$ and $(L \setminus L')[S'], S'' \mathcal{T} R$, which are immediate by definition of $\mathcal{T}$.
(b) $T \downarrow L_i[T_i'], T_i''$ with $i \in I$ and $\widehat{L} \subseteq \bigcap_{i \in I} \widehat{L}_i$ and, for every $K \subseteq I$:

$$\text{either } S' \mathcal{R} \sum_{k \in K} T_k' \text{ or } S'' \mathcal{R} \sum_{k \in J \setminus K} T_k''. \quad (A.1)$$

There are two subcases:

(b1) $R \downarrow M[R'], R''$ with $\widehat{L} \cap \widehat{M} \neq \emptyset$ and $\widehat{L} \subset \widehat{M}$. In this case we must prove $(L \cap M)[S'], S'' \mathcal{T} R$ and $(L \setminus M)[S'], S'' \mathcal{T} R$, which are immediate by definition of $\mathcal{T}$.
(b2) $R \downarrow M_j[R'_j], R''_j$ with $j \in J$ and $\widehat{L} \subseteq \bigcap_{j \in J} \widehat{M}_j$. There are again two subcases: (b2.1) there are $i, k$ such that $\widehat{L}_i \not\subseteq \widehat{M}_k$; (b2.2) the contrary of (b2.1). In case (b2.1) we apply the simulation case 4(a): it must be $(L_i \cap M_k)[T_i'], T_i'' \mathcal{S} R$ and $(L_i \setminus M_k)[T_i'], T_i'' \mathcal{S} R$. As far as $(L_i \cap M_k)[T_i'], T_i'' \mathcal{S} R$ is concerned, $\widehat{L} \subseteq \widehat{L}_i \cap \widehat{M}_k$. If $L_i \cap M_k$ is not contained in every $M_j$ we reiterate the argument (b2.1) on the schema $(L_i \cap M_k)[T_i'], T_i'' \mathcal{S} R$. We end up with a set of schemas $L_i[T_i'], T_i''$ with $i \in I$ such that $L_i[T_i'], T_i'' \mathcal{S} R$ and the case (b2.2) holds. From now on the arguments of the two cases are the same. We let $L_i' = L_i$. From $L_i[T_i'], T_i'' \mathcal{S} R$ we have: for every $K' \subseteq J$:

$$\text{either } T_i' \mathcal{S} \sum_{k \in K'} R_k' \text{ or } T_i'' \mathcal{S} \sum_{k \in J \setminus K'} R_k''. \quad (A.2)$$

Let $K \subseteq J$. Since $\widehat{L} \subseteq \bigcap_{j \in J} \widehat{M}_j$, we must prove:

$$\text{either } S' \mathcal{T} \sum_{k \in K} R_k' \text{ or } S'' \mathcal{T} \sum_{k \in J \setminus K} R_k''. \quad (A.3)$$

For every $i \in I$, the constraint (A.2) implies

$$\text{either } T_i' \mathcal{S}^+ \sum_{k \in J} R_k' \text{ or } T_i'' \mathcal{S}^+ \sum_{k \in J \setminus K} R_k''. \quad (A.4)$$

45
where the relation is \( S^+ \). Let \( H_K = \{ h \in I \mid T'_h, S^+ \sum_{k \in K} R'_{k} \} \). By definition \( H_K \subseteq I \) and \( T''_h, S^+ \sum_{k \in I \setminus K} R''_k \) for every \( h' \in I \setminus H_K \). The constraint \( (A.1) \) implies

\[
\text{either } S'^{+} \sum_{h \in H_K} T'_h \text{ or } S''^{+} \sum_{h \in I \setminus H_K} T''_h \tag{A.5}
\]

The constraint \( (A.3) \) follows from \( (A.5) \) and \( (A.4) \).

The case \( (b2.2) \) is similar to \( (b2.1) \) but we apply the simulation case 4.(b)

As regards the item 7, let \( R \) be a subschema relation such that \( S \ R \ T \) and \( S' \ R \ T' \). Let \( \bar{R} \) be the least relation that contains \( R \) and that is closed under reflexivity and under the following operation:

- if \( S \bar{R} T \), then \( S, R \bar{R} T, R \) and \( R, S \bar{R} R, T \).

The relation \( \bar{R} \) is a subschema relation. We demonstrate the case \( S, R \bar{R} T, R \) and omit the other one because trivial. Let \( S, R \downarrow R' \). If \( S \downarrow \emptyset \) and \( R \downarrow R' \) then, by \( S \bar{R} T \), we have \( T \downarrow \emptyset \) and \( T, R \downarrow R' \). We can conclude by reflexivity of \( \bar{R} \). If \( S \downarrow B, S' \), then \( R' = B, S', R \). From \( S \bar{R} T \) we have that \( T \downarrow B'_i, T'_i \) for \( 1 \leq i \leq n \), with \( B \subseteq B'_i \) and \( S' \bar{R} \sum_{1 \leq i \leq n} T'_i \). Hence \( T, R \downarrow B'_i, T'_i, R \) for \( 1 \leq i \leq n \) and now \( S', R \bar{R} \sum_{1 \leq i \leq n} T'_i, R \) by definition of \( \bar{R} \). The remaining cases are similar. We conclude by remarking that \( (S, S', T, T') \) is in the transitive closure of \( \bar{R} \).

As regards the item 9, let \( R \) be the least relation containing the identity and the pairs:

\[
(\text{Empty}, S), (S, \text{Any}), ((S)^*, \text{AnyChan}), ((\text{Any})^{10}, (S)^0), (\langle \text{Empty} \rangle^{10}, (S)^1), (S, (\text{int} + \text{string} + \text{AnyChan} + \sim[\text{Any}])^*), (n, \text{int}), (s, \text{string})
\]

The proof that \( R \) is a subschema relation is straightforward, except for the pairs \( (S, \text{Any}) \) and \( (S, (\text{int} + \text{string} + \text{AnyChan} + \sim[\text{Any}])^*) \). We analyze the first pair, the other being similar. We show that every \( R \) such that \( S \downarrow R \) is simulated by \( \text{Any} \). The interesting case is when \( R = L[S']^n, S'' \). In this case \( \text{Any} \downarrow \sim[\text{Any}], (\text{int} + \text{string} + \text{AnyChan} + \sim[\text{Any}])^* \) and we are in case 4.b of Definition 1. Since \( S \downarrow R \) then \( S \) is not-empty, similarly for \( \text{Any} \). Therefore we are reduced to \( (S', \text{Any}), (S'', (\text{int} + \text{string} + \text{AnyChan} + \sim[\text{Any}])^*) \in R \), which hold by definition. \( \Box \)
B Soundness of the static semantics

The basic statements below are standard preliminary results for the subject reduction theorem.

Lemma 8 (Weakening)  
1. If \( \Gamma \vdash E : S \) and \( x \notin \text{fv}(E) \), then \( \Gamma + x : T \vdash E : S \);
2. If \( \Gamma ; \Delta \vdash P \) and \( x \notin \text{fv}(P) \), then both (a) \( \Gamma + x : S ; \Delta \vdash P \) and (b) \( \Gamma + x : \langle S \rangle^n ; \Delta + x : \langle S \rangle^\text{IO} \vdash P \).

Actually, the premises of the second statement of Lemma 8 also entail \( \Gamma + x : S ; \Delta + x : S \vdash P \), but this property is never used in the following. When a local channel is created, the property that is used is (b). A somewhat converse statement of weakening is the following.

Lemma 9 (Strengthening)  
If \( \Gamma \vdash E : S \) and \( x \notin \text{fv}(E) \), then \( \Gamma \setminus x \vdash E : S \). Similarly, if \( \Gamma ; \Delta \vdash P \) and \( x \notin \text{fv}(P) \), then \( \Gamma \setminus x ; \Delta \setminus x \vdash P \).

The following proposition collects properties about judgments of values. We recall that \( \Gamma \) is channeled when it binds variables to channel schemas.

Proposition 10  
Let \( \Gamma \vdash V : S \).

1. If \( S = L[S'], S'' \), then \( L \) is a singleton;
2. If \( S \ll \langle T \rangle^\ast \), then \( V \) is a variable;
3. If \( \Gamma \) is channeled and \( S \ll T_1 + T_2 \), then either \( S \ll T_1 \) or \( S \ll T_2 \);
4. If \( S \ll T_1, T_2 \), then there exist \( V_1 \) and \( V_2 \) such that \( V = V_1 \oplus V_2 \) and \( \Gamma \vdash V_1 : S_1 \) and \( \Gamma \vdash V_2 : S_2 \) and \( S_1 \ll T_1 \) and \( S_2 \ll T_2 \);
5. If and \( S \ll T^\ast \), then either \( V = \emptyset \) or \( V = V_1 \oplus V_2 \) with \( V_1 \neq \emptyset \) and \( \Gamma \vdash V_1 : S_1 \) and \( \Gamma \vdash V_2 : S_2 \) and \( S_1 \ll T \) and \( S_2 \ll T^\ast \).

Proof: Item (1) follows from the definition of judgment for expressions.

Item (2) follows from the definitions of values (a void expression or a sequence of non-void values) and of judgment for expressions.

Regarding item (3), we proceed by induction on the derivation of \( \Gamma \vdash V : S \).

The base case are:

- \( S = \emptyset \). By definition of \( \ll \): we have either \( T_1 \downarrow \emptyset \) or \( T_2 \downarrow \emptyset \), then we conclude;
- \( S = \text{B} \). Since \( S \downarrow \text{B}, \emptyset \) we have three cases. If \( S \ll T_1 \) or \( S \ll T_2 \) we immediately conclude. Otherwise, by definition of \( \ll \), we obtain:
We conclude by taking
\[ T_1 \downarrow B_i, Q_i \quad B \subseteq B_i \quad 1 \leq i \leq n \] (B.1)
\[ T_2 \downarrow B_j, Q_j \quad B \subseteq B_j' \quad n + 1 \leq j \leq m \] (B.2)
\[ () \subset \sum_{1 \leq i \leq m} Q_i \] (B.3)

Since B.3 implies \( Q_k \downarrow () \) for some \( k \in \{1, \ldots, m\} \), we conclude \( S \subset B_k, Q_k \) by either B.1 or B.2.

- \( S = \langle S' \rangle^a \). Similar to the previous case.

The inductive cases are:

- \( S = B, S_1 \). If \( S \subset T_1 \) or \( S \subset T_2 \) we immediately conclude. Otherwise, by definition of \( \subset \), we have \( T_1 \downarrow B_i, Q_i \) with \( B \subseteq B_i \) for \( 1 \leq i \leq n \), and \( T_2 \downarrow B_j, Q_j \) with \( B \subseteq B_j' \) for \( n + 1 \leq j \leq m \) and \( S_1 \subset \sum_{1 \leq i \leq m} Q_i \). We conclude by the inductive hypothesis.

- \( S = \langle S_1 \rangle^a, S_2 \). Similar to the previous case.

- \( S = a[S_1], S_2 \). If \( S \subset T_1 \) or \( S \subset T_2 \) we immediately conclude. Otherwise, by definition of \( \subset \), we have \( T_1 \downarrow L_1[Q_i], Q_i' \) for \( 1 \leq i \leq n \), and \( T_2 \downarrow L_j[Q_j], Q_j' \) for \( n + 1 \leq j \leq m \). Since \( a \) is a singleton \( (4) \) of \( \subset \) applies. We assume by contradiction that \( a[S_1], S_2 \not\subset L_i[Q_i], Q_i' \) for any \( i \in \{1, \ldots, m\} \) (i.e. \( S_1 \not\subset Q_i, S_2 \not\subset Q_i' \) for any \( i \in \{1, \ldots, m\} \)). Then we choose \( J_i \) as follows:

1. \( J_1 = \emptyset \) implies \( S_2 \subset \sum_{i \in \{1, \ldots, m\}} Q_i' \) and, by the inductive hypothesis, there exists \( k_1 \) such that \( S_2 \subset Q'_{k_1} \);
2. \( J_{k_1} = \{k_1\} \), since \( S_1 \not\subset Q_{k_1} \), we have \( S_2 \subset \sum_{i \in \{1, \ldots, m\}\{k_1\}} Q_i' \) and, by the inductive hypothesis, there exists \( k_2 \neq k_1 \) such that \( S_2 \subset Q'_{k_2} \);
3. \( J_{k_1, k_2} = \{k_1, k_2\} \), since \( S_1 \not\subset Q_{k_1} \) and \( S_1 \not\subset Q_{k_2} \), by the inductive hypothesis we have \( S_1 \not\subset Q_{k_1} + Q_{k_2} \). Then we must have \( S_2 \subset \sum_{i \in \{1, \ldots, m\}\{k_1, k_2\}} Q_i' \) that implies, by the inductive hypothesis, \( k_3 \) with \( k_3 \neq k_1 \) and \( k_3 \neq k_2 \) such that \( S_2 \subset Q'_{k_3} \);

\(\ldots\)

\((m + 1) J_{k_1, k_2, \ldots, k_m} = \{1, \ldots, m\} \) then we have to prove \( S_1 \subset \sum_{i \in \{1, \ldots, m\}} Q_i \) that, by inductive hypothesis, implies \( S_1 \subset Q_k \) for some \( k \in \{1, \ldots, m\} \).

But this is not possible because of the previous \( m \) judgements \( (S_1 \not\subset Q_{k_1} \) for \( (1) \), \( S_1 \not\subset Q_{k_2} \) for \( (2) \), \ldots, \( S_1 \not\subset Q_{k_m} \)\).

Therefore we obtain \( a[S_1], S_2 \not\subset T_1 + T_2 \) which contradicts the hypothesis.

- If \( S = a[S_1], \) since \( S \subset a[S_1], \emptyset \) we reduce to the previous case.

Regarding item (4), we proceed by induction on \( V \). For the base case assume that \( T_1 \downarrow \emptyset \) and \( S \subset T_2 \) (notice that this case includes the one where \( V = \emptyset \)). We conclude by taking \( V_1 = \emptyset \) and \( V_2 = V \). For the inductive case assume that either \( T_1 \downarrow R \) implies \( R \neq \emptyset \) or that \( T_1 \downarrow \emptyset \) and \( S \not\subset T_2 \). We reason by cases on the structure of \( V \), we only show the case when \( V = b, V' \), the others are similar. We have \( a = b, S' \) where \( \Gamma \vdash V : S' \). We must have \( T_1 \downarrow b, T_1' \) with \( b \subset b \) and \( S' \subset T_1', T_2 \). By induction hypothesis there exist \( V_1' \) and \( V_2 \) such that \( V' = V_1' \sharp V_2 \) and \( \Gamma \vdash V_1' : S_1' \) and \( \Gamma \vdash V_2 : S_2 \) and \( S_1' \subset T_1' \) and

48
$S_2 <: T_2$. We conclude by taking $V_1 = b, V'_1$.

Regarding item (5), if $V = ()$ we conclude immediately. Assume $V \neq ()$. Then we must have $T \downarrow R$, with $R \neq ()$ and $S <: R, T^\ast$. By item (4) we obtain $V = V_1@V'_2$ and $\Gamma \vdash V_1 : S_1$ and $\Gamma \vdash V_2 : S_2$ and $S_1 <: R$ and $S_2 <: T^\ast$. Since $R$ is a handle and $R \neq ()$ we must have $V_1 \neq ()$. Furthermore, since $R$ is a handle of $T$, we have $R <: T^\ast$. Hence we conclude $S_1 <: T^\ast$.

Lemma 11 (Substitution) Let $V$ be a dom($\Gamma$)-value and $\Gamma \vdash V : S$.

(1) If $\Gamma \vdash E : T$, $\Gamma \vdash x : R$ and $S <: R$, then $\Gamma \vdash E\{V/_{_{x}}\} : T'$ with $T' <: T$.

(2) If $\Gamma; \Delta \vdash P$, $\Gamma + \Delta \vdash x : R$ and $S <: R$, then $\Gamma; \Delta \vdash P\{V/_{_{x}}\}$.

Proof: The proof is by induction on the structure of the derivations of $\Gamma \vdash E : T$ and $\Gamma; \Delta \vdash P$.

For (1) we only discuss the case when $E$ is a sequence $E_1, E_2$. By definition of $\vdash$, $\Gamma \vdash E_1 : T_1$ and $\Gamma \vdash E_2 : T_2$, and by inductive hypothesis we have

\[
\begin{align*}
\Gamma \vdash E_1\{V/_{_{x}}\} : T'_1 \quad & \text{and} \quad T'_1 <: T_1 \quad \text{(B.4)} \\
\Gamma \vdash E_2\{V/_{_{x}}\} : T'_2 \quad & \text{and} \quad T'_2 <: T_2 \quad \text{(B.5)}
\end{align*}
\]

From (B.4), and (B.5) we obtain $\Gamma \vdash (E_1, E_2)\{V/_{_{x}}\} : T'_1, T'_2$. By Proposition 2(6), $T'_1, T'_2 <: T_1, T_2$ and we conclude.

For (2) we only discuss the case when the last rule is (out). Then $P = u!(E)$ and the premises of the rule are the judgments $\Gamma \vdash E : T$ and $\Gamma; \Delta \vdash u : R$, and the predicate

\[
R <: (T)^\circ \quad \text{(B.6)}
\]

We must prove $\Gamma; \Delta \vdash u!(E)\{V/_{_{x}}\}$. By $\Gamma \vdash E : T$, the hypothesis $\Gamma \vdash V : S$, $S <: R$, and the substitution lemma for expressions, we obtain

\[
\begin{align*}
\Gamma \vdash E\{V/_{_{x}}\} : T' \quad \text{(B.7)} \\
T' <: T \quad \text{(B.8)}
\end{align*}
\]

As regards the subject of the output, there are two subcases: (a) $x \neq u$ and (b) $x = u$. Case (a) follows by (B.6), (B.8), contravariance of $\langle \cdot \rangle^\circ$ and transitivity of $<:$: Case (b) implies $S = R$. Therefore, by Proposition 10, $V$ is a variable. The lemma follows by (B.7), the hypotheses $\Gamma \vdash x : S$, the (B.6), the contravariance of $\langle \cdot \rangle^\circ$, and the transitivity of $<:$.

\[\square\]

The weakening, strengthening, and substitution lemmas entail a subsumption property that is useful for the correctness of the rule (dtr1) in the subject
reduction.

**Proposition 12** If $\Gamma + x : T; \Delta \vdash P$ and $x \notin \text{dom}(\Delta)$ and $S <: T$ then $\Gamma + x : S; \Delta \vdash P$.

In the rest of this appendix, we generalize all the functions defined over patterns to markers and to sequences of patterns and markers $\Phi = F_1 :: F_2 :: \cdots :: F_n$ where a marker is treated like the empty sequence $()$ and a sequence $F_1 :: F_2 :: \cdots :: F_n$ is treated like the pattern $F_1, F_2, \ldots, F_n$ which reduces to $(())$ when $n = 0$. In particular, we generalize the functions $\text{schof}()$, $\text{fv}()$, $\text{Env}()$. The next two statements regard the soundness of the evaluation of expressions and of pattern matching. Straightforward proofs are omitted.

**Lemma 13 (Evaluation)** Let $\Gamma \vdash E : S$. If $E \Downarrow \text{dom}(\Gamma) V$, then $\Gamma \vdash V : T$ and $T <: S$.

**Lemma 14 (Pattern Matching)** Let $\Gamma \vdash V : S$ and $\Gamma \vdash V \in \Phi \leadsto \sigma$.

1. $S <: \text{schof}(\Phi)$;
2. If $u \notin \text{fv}(V)$, then $\Gamma + u : S \vdash V \in \Phi \leadsto \sigma$;
3. for every $u \in \text{fv}(\Phi)$, $\Gamma \vdash \sigma(u) : T$ and $T <: \text{Env}(\Phi)(u)$.

**Proof:** items (1) and (2) are trivial. Regarding item (3), we proceed by induction on the proof tree of $\Gamma \vdash V \in \Phi \leadsto \sigma$. The only interesting case is when the last rule in the proof of $\Gamma \vdash V \in \Phi \leadsto \sigma$ is (PM7):

\[
\frac{\frac{\Gamma \vdash V \in F :: x/V :: \Phi' \leadsto \sigma'}{\Gamma \vdash V \in (x : F) :: \Phi' \leadsto \sigma}}{(\text{pm7})}
\]

and take $u = x$. Eventually, in the proof tree of $\Delta \vdash V \in F :: x/V :: \Phi' \leadsto \sigma$, there will be an application of rule (PM5):

\[
\frac{\frac{\Gamma \vdash V' \in \Phi' \leadsto \sigma'}{V = V'' \circ V'}}{(\text{pm3})}
\]

By letting $\Phi' = [\ ]$ and $V' = ()$ and $\sigma' = \emptyset$ we obtain a proof tree of $\Gamma \vdash V'' \in (x : F) \leadsto \sigma''$. From item (1) we derive that $\Gamma \vdash V'' : S$ implies $S <: \text{schof}(F)$. We conclude by observing that $\text{Env}(\Phi)(x) = \text{schof}(F)$ and that $\sigma(x) = V''$. $\Box$

Every preliminary is set for the subject reduction. For readability sake we recall the statement.

**Theorem 6 (Subject Reduction)** Let $\Gamma; [\Gamma]_1^{\text{IO}} \vdash P$. Then
(1) if $\Gamma \vdash_1 P \xrightarrow{(\Gamma')u_1(V)} Q$, then (a) $\Gamma + \Gamma'$; $[\Gamma + \Gamma']^{10}_2 \vdash Q$, (b) $\Gamma + [\Gamma']^{10}_2 \vdash u : S$, $\Gamma + \Gamma' \vdash V : T$ and $S < : (T)^0$;

(2) if $\Gamma \vdash_1 P \xrightarrow{u \cdot (F)} Q$, then (a) $(\Gamma'; [\Gamma]'^{10}) + \text{Env}(F) \vdash Q$ and (b) $\Gamma + [\Gamma']^{10}_2 \vdash u : S$ with $S < : (\text{name}(F))^1$;

(3) if $\Gamma \vdash_1 P \xrightarrow{(\Gamma')u \rightarrow v} Q$, then (a) $\Gamma + \Gamma'$; $[\Gamma + \Gamma']^{10}_2 \vdash Q$ and (b) $\Gamma \setminus \text{dom}(\Gamma + \Gamma')^{10}_2 \vdash u : S$, $\Gamma + \Gamma' \vdash v : (T)^0$ and $S < : (T)^2$;

(4) if $\Gamma \vdash_1 P \xrightarrow{(u \oplus \eta ; : (S)^{10}_2)} Q$, then $(\Gamma; [\Gamma]'^{10}) + u : (S)^{10}_2 \vdash Q$;

(5) if $\Gamma \vdash_1 P \xrightarrow{=} Q$, then $\Gamma; [\Gamma]'^{10}_1 \vdash Q$.

Let $\vdash M$. Then

(6) if $M \xrightarrow{\Delta} N$, then $\vdash N$.

Proof: The proof proceeds by induction on the structure of the derivation of $\Gamma \vdash_1 P \xrightarrow{=} Q$ and by cases on the last rule that has been applied for the first five items. Item (6) is similar, but the induction is on the structure of the derivation of $\vdash M$. We omit the cases that are straightforward.

When the last rule is an instance of (TR4) we have:

$$\begin{align*}
\Gamma + v : \langle S \rangle^\kappa \vdash_1 P \xrightarrow{(\Gamma')u_1(V)} Q & \quad v \neq u \quad v \in \text{fv}(V) \setminus \text{dom}(\Gamma') \\
\Gamma \vdash_1 \text{new } v : \langle S \rangle^\kappa \text{ in } P \xrightarrow{(\Gamma' + v \cdot : (S)^{\kappa})u_1(V)} Q
\end{align*}$$

By inductive hypotheses applied to $\Gamma + v : \langle S \rangle^\kappa \vdash_1 P \xrightarrow{(\Gamma')u_1(V)} Q$ we obtain

$$\begin{align*}
\Gamma + v : \langle S \rangle^\kappa + \Gamma' & \quad [\Gamma + v : \langle S \rangle^\kappa + \Gamma']^{10}_2 \vdash Q \quad \text{(B.9)} \\
\Gamma + v : \langle S \rangle^\kappa + \Gamma' & \vdash u : S' \quad \text{(B.10)} \\
\Gamma + v : \langle S \rangle^\kappa + \Gamma' & \vdash V : T \quad \text{(B.11)} \\
S' & < : (T)^0 \quad \text{(B.12)}
\end{align*}$$

The conclusion (a) follows from (B.9); the conclusion (b) follows by (B.10), (B.11), and (B.12) because $u \neq v$.

When the last rule is an instance of (TR5) we have:

$$\begin{align*}
\xrightarrow{(\text{TR5})} E \downarrow V \quad (\Gamma \vdash V \not\in F_i)^{i \in 1..j-1} \quad \Gamma \vdash V \in F_j \sim \sigma \\
\Gamma \vdash_1 \text{match } E \text{ with } \{ F_i \Rightarrow P_i^{i \in 1..n} \} \xrightarrow{P_j \sigma}
\end{align*}$$

By the hypothesis $\Gamma; [\Gamma]'^{10}_1 \vdash P$, Lemma 13, and rule (MATCH) we have:

$$\Gamma; [\Gamma]'^{10}_1 \vdash V : S \quad S < : \sum_{i \in 1..n} \text{schof}(F_i) \quad \text{(B.13)}$$
By Lemma 14 applied to \( \Gamma \vdash V \in F \sim \sigma \) and (B.13) we obtain that, for every \( v \in \text{fv}(F) \), \( \Gamma + \Gamma' \vdash \sigma(v) : T' \) and \( T' \triangleleft : \text{Env}(F)(v) \). By Lemma 11 applied to this last judgment, we derive \( \Gamma ; [\Gamma]^{10}_1 \vdash P_j \sigma \).

When the last rule is an instance of \((\text{tr8})\) we have:

\[
\Gamma \vdash \text{spawn} \{P\} \quad Q \quad \frac{\Gamma \vdash \text{spawn} \{P\} \quad Q \quad \text{new} \quad \text{in spawn} \{P'\} \quad Q' \sigma}{\text{P}^{(\Gamma)u_1(V)} \quad \frac{\Gamma \vdash P^{(\Gamma)u_1(V)} \quad \Gamma \vdash Q^{u?(F)} \quad \text{dom}(\Gamma') \cap \text{fv}(Q) = \emptyset \quad \Gamma + \Gamma' \vdash V \in F \sim \sigma}{\Gamma + \Gamma' \vdash V : T}}
\]

By inductive hypotheses on \( \Gamma \vdash P^{(\Gamma)u_1(V)} \) and \( \Gamma \vdash Q^{u?(F)} \) we have:

\[
\begin{align*}
\Gamma + \Gamma' ; [\Gamma + \Gamma']^{10}_1 & \vdash P' \tag{B.14} \\
\Gamma + \Gamma' & \vdash V : T \tag{B.15} \\
\Gamma + \Gamma' \vdash u : S & \quad S \triangleleft : \langle \text{schof}(F) \rangle^1 \quad S \triangleleft : \langle T \rangle^0 \tag{B.16} \\
(\Gamma ; [\Gamma]^{10}_1) + \text{Env}(F) & \vdash Q' \tag{B.17}
\end{align*}
\]

By Lemma 14 applied to \( \Gamma + \Gamma' \vdash V \in F \sim \sigma \), (B.15), and (B.16) we obtain that, for every \( v \in \text{fv}(F) \), \( \Gamma + \Gamma' \vdash \sigma(v) : T' \) and \( T' \triangleleft : \text{Env}(F)(v) \). By Lemma 11 applied to this last judgment, (B.16), and (B.17) we derive \( (\Gamma ; [\Gamma]^{10}_1) + \Gamma' \vdash Q' \sigma \). We conclude with (B.14), (spawn), and (new).

The case \((\text{tr10})\) is omitted because the resulting process is complex and the demonstration requires a long uninteresting analysis of the proof tree.

When the last rule is an instance of \((\text{dtr1})\) we have:

\[
\begin{align*}
\Delta = v_i : S_i^{i \in I} & \quad \langle \text{dtr8} \rangle \quad \frac{\Gamma \vdash \text{spawn} \{u!1(V)\} \quad \Gamma + \Delta \vdash \Gamma + \Delta \vdash_1 \text{spawn} \{u!1(V)\} \quad \text{R}}{\Gamma \vdash P \quad \frac{\Gamma + \Gamma' : \text{V} \vdash_1 \text{R}}{\Delta \vdash_1 \Gamma \vdash \Gamma + \Gamma' \vdash Q \quad \Delta \vdash_1 \Gamma \vdash \Gamma + \Gamma' \vdash \text{spawn} \{u!(V)\} \quad \text{R}}}
\end{align*}
\]

In order to prove \( \vdash (\Gamma + v_i : S_i^{i \in I} \vdash_1 Q \quad \Gamma + \Delta \vdash \text{spawn} \{u!(V)\} \quad \text{R}) \) we may reduce to demonstrate

\[
\begin{align*}
\Gamma + v_i : S_i^{i \in I} & \vdash Q \tag{B.18} \\
\Gamma + \Delta & \vdash [\Gamma']^{10}_1 \vdash \text{spawn} \{u!(V)\} \quad \text{R} \tag{B.19}
\end{align*}
\]

because the machine consistency follows by definition of meet and the fact that \( v_i \) are fresh. (We notice that, by definition of \( \Delta, [\Gamma' + \Delta]^{10}_1 = [\Gamma']^{10}_1 \).) The judgment (B.18) and

\[
\begin{align*}
\Gamma + [\Gamma]^{10}_1 & \vdash u : S \tag{B.20} \\
\Gamma + v_i : S_i^{i \in I} & \vdash V : T \quad S \triangleleft : \langle T \rangle^0 \tag{B.21}
\end{align*}
\]

52
are a consequence of the inductive hypothesis on $\Gamma \vdash l \Gamma P \varepsilon Sii \in I u! (V) \rightarrow Q$. As regards (B.19), by $\vdash M$ we derive $\Gamma' \vdash \Gamma'$ and $\Gamma [\Gamma']_{10} \vdash R$ and by Lemma 8 and Proposition 12 we obtain $\Gamma' + \Delta ; [\Gamma']_{10} \vdash R$. To demonstrate $\Gamma' + \Delta ; [\Gamma']_{10} \vdash u! (V)$ we reason as follows ((B.19) is entailed by (spawn) applied to these last judgments). By (B.20), $u@I'$, and the well-typedness of $M$, we derive $\Gamma' \vdash l \Gamma' R \rightarrow \Gamma + u : \langle S \rangle 10 \vdash \langle S \rangle 10 + u : \langle S \rangle 10 \vdash \langle S \rangle 10$. To demonstrate $\Gamma' + \Delta ; [\Gamma']_{10} \vdash u! (V)$, we reason as follows ((B.19) is entailed by (spawn) applied to these last judgments). By (B.21), Lemmas 8 and 9 and Proposition 12 we obtain $\Gamma' \vdash \Gamma' + u : \langle S \rangle 10 \vdash \langle S \rangle 10 + u : \langle S \rangle 10 \vdash \langle S \rangle 10$. The judgment (B.19) follows from (B.22) and (B.23) with the rule (out).

When the last rule is an instance of (dtr2) we have:

\[
\begin{array}{c}
\Gamma \vdash_{1} P \left(\begin{array}{c}
u \in I \langle S \rangle 10 \vdash Q \\
\nu \notin \text{dom}(\Gamma') \cup \text{dom}(\Gamma)
\end{array}\right) \\
\Gamma \vdash_{1} P \parallel \Gamma' \vdash_{1} R \\
\rightarrow \\
\Gamma + u : \langle S \rangle 10 \vdash \langle S \rangle 10 + u : \langle S \rangle 10 \vdash \langle S \rangle 10 + u : \langle S \rangle 10 + u : \langle S \rangle 10 + u : \langle S \rangle 10
\end{array}
\]

We verify the well-typedness of the two runtime environments; machine consistency is immediate. By the inductive hypothesis on $\Gamma \vdash l \Gamma P \varepsilon Sii \in I u! (V) \rightarrow Q$, we obtain $\Gamma ; [\Gamma]_{10} + u : \langle S \rangle 10 \vdash Q$. This is sufficient for the correctness of location $l$ because $\Gamma ; [\Gamma]_{10} + u : \langle S \rangle 10 = (\Gamma + u : \langle S \rangle 10) ; [\Gamma + u : \langle S \rangle 10]_{10}$. The judgment $(\Gamma' + u : \langle S \rangle 10) ; [\Gamma' + u : \langle S \rangle 10]_{10} \vdash R$ follows by Lemma 8 applied to $\Gamma'$; $[\Gamma']_{10} \vdash R$.

When the last rule is an instance of (dtr3) we have

\[
\begin{array}{c}
\Gamma \vdash_{1} P \left(\begin{array}{c}
u \in I \langle S \rangle 10 \vdash Q \\
\nu \notin \text{dom}(\Gamma') \cup \text{dom}(\Gamma)
\end{array}\right) \\
\Gamma \vdash_{1} P \parallel \Gamma' \vdash_{1} R \\
\rightarrow \\
\Gamma + u : \langle S \rangle 10 \vdash \langle S \rangle 10 + u : \langle S \rangle 10 \vdash \langle S \rangle 10 + u : \langle S \rangle 10
\end{array}
\]

We focus on the well-typedness of the two runtime environments. By inductive hypothesis on $\Gamma \vdash_{1} P \left(\begin{array}{c}
u \in I \langle S \rangle 10 \vdash Q \\
\nu \notin \text{dom}(\Gamma') \cup \text{dom}(\Gamma)
\end{array}\right)$ we obtain

\[
\begin{align*}
\Gamma + \Gamma'' & ; [\Gamma + \Gamma'']_{10} \vdash Q \\
\Gamma + \Gamma'' & \vdash u : T \\
\Gamma + \Gamma'' & \vdash v : \langle T \rangle 0 \\
T & \vdash : \langle T \rangle 1
\end{align*}
\]

By (B.24) we immediately derive that the left runtime environment is well-typed. Therefore we focus on the right runtime environment. To demonstrate
the correctness of its process we will eventually use (SPAWN). Therefore we reduce to prove: (1) \( \Gamma' + \Gamma''; [\Gamma' + \Gamma'']_1^{\top} \vdash R \) and (2) \( \Gamma' + \Gamma''; [\Gamma' + \Gamma'']_1^{\top} \vdash u?x : S)v!(x) \). The judgment (1) follows by the hypothesis \( \Gamma'; [\Gamma']_1^{\top} \vdash R \), \( \text{dom}(\Gamma') \cap \text{dom}(\Gamma') = \emptyset \), by Lemma 8 and (in case \( v \in \text{dom}(\Gamma') \)) Proposition 12.

As regards (2), the well-typedness of \( M \) entails \( \langle S \rangle^\kappa : T \). By transitivity of \( \vdash \), \( \langle S \rangle^\kappa : \langle T \rangle^I \). Therefore \( \kappa \) is either \( 1 \) or \( 10 \) and \( S : \langle T \rangle^I \). Without loss of generality, let \( x \) be fresh. Since \( \Gamma + \Gamma'' = \Gamma + \Gamma'' \), (B.26) and Lemma 8 give \( \Gamma' + \Gamma'' + x : S \vdash v : \langle T \rangle^0 \). Then, by rule (OUT), we obtain \( \Gamma' + \Gamma'' + x : S; [\Gamma' + \Gamma'' + x : S]_1^{\top} \vdash v! (x) \). Finally, it is easy to derive \( \Gamma' + \Gamma'' + [\Gamma' + \Gamma'']_1^{\top} \vdash u : \langle S \rangle^\kappa \) from the hypothesis \( \Gamma' + u : \langle S \rangle^\kappa \). We conclude with (SELECT).

When the last rule is an instance of (DTR5) we have:

\[
(\text{dtr5}) \quad \frac{M \quad \Delta \rightarrow N \quad (\text{dom}(N) \setminus \text{dom}(M)) \cap \text{dom}(\Gamma) = \emptyset \quad \Delta @ 1 \subseteq \Gamma}{M \parallel \Gamma \vdash P \quad \Delta @ 1 \Rightarrow N \parallel \Gamma \vdash P}
\]

Since \( \vdash (M \parallel \Gamma \vdash P) \) then both \( 1 \) \( \vdash M \) and \( 2 \) \( \vdash (\Gamma \vdash P) \). By inductive hypotheses applied to \( 1 \) and \( M \rightarrow N \) we derive \( \vdash N \). The machine consistency of the composite machine follows from that of \( \vdash (M \parallel \Gamma \vdash P) \) and the constraint \( \Delta @ 1 \subseteq \Gamma \).

The proof of the Progress Theorem follows.

**Theorem 7 (Progress)** Let \( \Gamma \) be channeled.

1. If \( \Gamma \vdash V : S \) and \( S \vdash \text{cho}(F) \), then there is \( \sigma \) such that \( \Gamma \vdash V \in F \sim \sigma \);
2. If \( \Gamma ; [\Gamma']_1^{\top} \vdash P \) and \( \Gamma \vdash_1 P \overset{(\Gamma')u!}{\sim} Q' \) and \( \Gamma \vdash_1 P \overset{u?V}{\sim} Q'' \), then there is \( Q \) such that \( \Gamma \vdash_1 P \overset{u}{\sim} Q \);
3. If \( \vdash (\Gamma \vdash P \parallel M) \), \( \Gamma \vdash_1 P \overset{(\Gamma')u!}{\sim} Q \), and \( u \) is located at a location of \( M \), then \( \Gamma \vdash_1 P \parallel M \rightarrow_{\Delta} \Gamma \vdash_1 Q \parallel N \), for some \( N \). Similarly when the label is \( (\Gamma')u \sim v \).

**Proof:** As regards item (1), let the size of a pattern \( F \), written \( h(F) \), be defined as follows:

\[
\begin{align*}
h() &= h(B) = h(\langle S \rangle^\kappa) = h(L[F]) = 1 \\
h(S^\kappa) &= 1 + h(S) \\
h(x : F) &= 2 + h(F) \\
h(F_1, F_2) &= h(F_1 + F_2) = 1 + h(F_1) + h(F_2) \\
h(Y) &= 1 + h(F(Y))
\end{align*}
\]

Notice that \( h(F) \) is well-defined when \( F \) is a well-formed pattern because a pattern name \( Y \) cannot occur unguarded in \( F(Y) \) and \( L[F] \) has size 1 regardless...
of \( F \)'s size. We generalize the \( h \) function to markers and to sequences of patterns and markers, where the size of a marker is 1 and the size of a sequence \( \Phi = F_1 :: F_2 :: \cdots :: F_n \) is defined as the sum of the sizes of all of its elements.

The proof is by induction on the pair \((V, h(\Phi))\), the idea being that at each induction step either we reduce to pattern matching a value that is structurally smaller than \( V \) or the size of the pattern sequence decreases. Recall that, since \( S \) is the schema of a value, it does not contain \(^+\)'s, starred schemas, and schema names, except possibly within channel constructors.

We only show the most relevant cases. In the base case we have \( h(\Phi) = 0 \) and \( V = \emptyset \). We conclude immediately by (PM1). Assume \( h(\Phi) > 0 \), meaning that \( \Phi = F :: \Phi' \) for some \( F \) and \( \Phi' \). We reason by cases on the structure of \( F \).

Assume \( F = () \). We notice that \( \text{schof}(\Phi) <: \text{schof}(\Phi') \) and that \( h(\Phi') < h(\Phi) \). By induction hypothesis we obtain \( \Gamma \vdash V \in \Phi' \rightsquigarrow \sigma \) from which we conclude by (PM2).

Assume \( F = L[F'] \). Then \( V = a[V']@V'' \) where \( a \in L, \Gamma \vdash V' : S', \Gamma \vdash V'' : S'', S' <: \text{schof}(F'), \) and \( S'' <: \text{schof}(\Phi') \). By induction hypothesis we obtain \( \Gamma \vdash V' \in F' \rightsquigarrow \sigma \) and \( \Gamma \vdash V'' \in \Phi' \rightsquigarrow \sigma' \) and we conclude by (PM6).

Assume \( F = F_1 + F_2 \). Notice that \( \text{schof}(\Phi) <: \text{schof}(F_1 :: \Phi') + \text{schof}(F_2 :: \Phi') \). By Proposition 10(3) we have that either \( S <: \text{schof}(F_1 :: \Phi') \) or \( S <: \text{schof}(F_2 :: \Phi') \). If \( S <: \text{schof}(F_1 :: \Phi') \) then by induction hypothesis \( \Gamma \vdash V \in F_1 :: \Phi' \rightsquigarrow \sigma \) and we conclude by (PM8). If \( S \not<: \text{schof}(F_1 :: \Phi') \) then by Lemma 14(1) we have \( \Gamma \vdash V \not\in F_1 :: \Phi' \). From \( S <: \text{schof}(F_2 :: \Phi') \) and the induction hypothesis we obtain \( \Gamma \vdash V \in F_2 :: \Phi' \rightsquigarrow \sigma \) from which we conclude by (PM9).

Assume \( F = T^* \). Let \( V = V_1 @ V_2 \) so that \( \Gamma \vdash V_1 : S_1 \) and \( \Gamma \vdash V_2 : S_2 \) and \( S_1 <: T^* \) and \( S_2 <: \text{schof}(\Phi') \). We take \( V_1 \) to be the longest prefix of \( V \) with these properties. The existence of \( V_1 \) and \( V_2 \) is guaranteed by Proposition 10(4). By induction hypothesis we obtain that \( \Gamma \vdash V_2 \in \Phi' \rightsquigarrow \sigma \).

Now we reason on the structure of \( V_1 \) to show that there exists \( n \geq 0 \) such that \( \Gamma \vdash V_1 \in T^n \rightsquigarrow \emptyset \). Assume \( V_1 = \emptyset \). Then it is sufficient to take \( n = 0 \). Assume \( V_1 \neq \emptyset \). By Proposition 10(5) there exist \( V_1' \) and \( V_1'' \) such that \( V_1' \neq \emptyset \) and \( \Gamma \vdash V_1' : S_1' \) and \( \Gamma \vdash V_1'' : S_1'' \) and \( S_1' <: T \) and \( S_1'' <: T^* \). By induction hypothesis we obtain that \( \Gamma \vdash V_1' \in T \rightsquigarrow \emptyset \) and furthermore there exists \( m \geq 0 \) such that \( \Gamma \vdash V_1'' \in T^m \rightsquigarrow \emptyset \) and now it is sufficient to take \( n = m + 1 \) and we conclude by noticing that if \( \Gamma \vdash V_1' \in T \rightsquigarrow \emptyset \) and \( \Gamma \vdash V_1'' \in T^m \rightsquigarrow \emptyset \), then \( \Gamma \vdash V_1' @ V_1'' \in T, T^m \rightsquigarrow \emptyset \).

Because \( V_1 \) was chosen as the longest prefix of \( V \) such that \( S_1 <: T^* \) and \( S_2 <: \text{schof}(\Phi') \), by soundness of pattern matching (Lemma 14(1)) we conclude that
any extension of $V_1$ with a nonempty suffix $W$ such that $V_2 = W @ V'_2$ will lead us to conclude either $\Gamma \vdash V_1 @ W \not\in T^*$ or $\Gamma \vdash V'_2 \not\in \Phi'$. Hence we conclude by (pm12).

As regards item (2), by Theorem 6(1) applied to $\Gamma; [\Gamma_1]^{10} \vdash P$ and $\Gamma; [\Gamma_1]^{10} \vdash_{(V_2)} P \rightarrow_{(V)} Q'$, we derive $\Gamma + [\Gamma_1]^{10} \vdash u : S$, $\Gamma + \Gamma' \vdash V : T$ and $S \prec \langle T \rangle^0$. By Theorem 6(2) applied to $\Gamma; [\Gamma_1]^{10} \vdash P$ and $\Gamma; [\Gamma_1]^{10} \vdash_{(V)} P \rightarrow_{(F)} Q''$, we also derive $\Gamma + [\Gamma_1]^{10} \vdash u : S$ and $S \prec \langle \text{schof}(F) \rangle^1$. Since $\Gamma$ is channeled, $S = \langle S' \rangle^\kappa$, for some $S'$, $\kappa$, and by Proposition 2, $T \prec \langle \text{schof}(F) \rangle$. Therefore, by item 1, there is $\sigma$ such that $\Gamma + \Gamma' \vdash V \in F \sim \sigma$. The proof now requires a close inspection of the proof trees of $\Gamma \vdash_{(p_3)} P$ and $\Gamma \vdash_{(p_6)} P' \rightarrow_{(V)} Q$, by definition of the transition relation, these trees must have common subtrees beginning at the root and terminating in correspondence of a subterm $\text{spawn} \{P'\} P''$ of $P$. At this point, the two subtrees continue with premises $\Gamma + \Gamma'' \vdash P' \rightarrow_{(V)} Q'_1$ and $\Gamma + \Gamma'' \vdash P'' \rightarrow_{(F)} Q''_2$ (or conversely). Progress holds because rule (tr8) may be applied (the constraint $\text{dom}(\Gamma'') \cap \text{fv}(P'') = \emptyset$ may be easily enforced by alpha-conversion) to $\text{spawn} \{P'\} P''$ and the resulting $\tau$-transition may be lifted to $P$ by means of rules (tr3), (tr6), (tr7).

Item (3) is straightforward. □

C The subschema relation and the type system

The definition of $\prec$ in Section 4 is given coinductively and it is hard to implement directly. In this section we illustrate the algorithm used in PiDuce for $\prec$ and we demonstrate its soundness and completeness. The algorithm follows the style of Hosoya, Pierce and Vouillon [22] has an exponential computational cost (in the sizes of the argument schemas). In order to alleviate this cost we define a subclass of schemas and demonstrate the existence of a polynomial algorithm for them.

Let $\text{handles}(S) = \{R \mid S \downarrow R\}$ and let $\varphi(1..n)$ be the set of subsets of numbers in 1..n. Table C.1 contains the inference rules that define a relation $S \preceq_k T \Rightarrow \mathcal{A}'$, which we are going to relate with $\prec$. The set $\mathcal{A}$, called assumptions, is a set of pairs $(S,T)$ representing relations that have been proved or that are being proved. The set $\mathcal{A}'$, following Brand and Henglein [9], is used for recording already computed or being computed relations. The rules parse the structure of handles of the left schema. Rule (empty) accounts for left schemas with no handle (empty schemas). Rules (void), (base), (chan), (split), and (lseq) deal with schemas that are handles (void, sequences with an initial schema that is either basic or channel or labelled). They closely correspond to the items 1,
The algorithmic subschema (arguments of shape B) are always replaced by B, (). Similarly for \( \langle S \rangle, L[S], S + S', U, \) and \( S^* \). Arguments () \( S \) are always replaced by \( S \).

<table>
<thead>
<tr>
<th>(empty)</th>
<th>(void)</th>
<th>(base)</th>
</tr>
</thead>
<tbody>
<tr>
<td>handles((S) = \emptyset)</td>
<td>( T \downarrow () )</td>
<td>( (T \downarrow B_i, T_i \mid B_i \subseteq B)<em>{i \in 1..n} S \leq_h \sum</em>{i \in 1..n} T_i \Rightarrow A' )</td>
</tr>
<tr>
<td>( S \leq_h T \Rightarrow A )</td>
<td>( (\emptyset \leq_h T \Rightarrow A) )</td>
<td>( B, S \leq_h T \Rightarrow A' )</td>
</tr>
</tbody>
</table>
| (chan) | \( (T \downarrow (T_i)^{\kappa_i}, T_i')_{i \in 1..n} \kappa \leq \kappa_i \) | \(\left\{ \begin{array}{l}
\kappa_i = 0 \quad \text{implies} \quad T_i \geq_h S \Rightarrow \text{A} \\
\kappa_i = 1 \quad \text{implies} \quad S \leq_h T_i \Rightarrow \text{A} \\
\end{array} \right. \) |
| \( \left( \begin{array}{l}
\kappa_i = 0 \quad \text{implies} \quad T_i \geq_h S \Rightarrow \text{A} \\
\kappa_i = 1 \quad \text{implies} \quad S \leq_h T_i \Rightarrow \text{A} \\
\end{array} \right) \) | \( S' \leq_h \sum_{i \in 1..n} T_i' \Rightarrow A_{n+1} \) | \( \langle S \rangle, S' \leq_h T \Rightarrow A_{n+1} \) |
| (split) | \( (L \setminus L'[S], S') \leq_h T \Rightarrow A' \) | \( L[S], S' \leq_h T \Rightarrow A'' \) |
| (lseq) | \( (T \downarrow L[T], T'') \quad \hat{L} \subseteq \hat{L}' \quad \hat{L} \cap \hat{L}' \neq \emptyset \) | \( L[S], S' \leq_h T \Rightarrow A'' \) |
| \( \left( \begin{array}{l}
\hat{L} \subseteq \bigcap_{i \in 1..n} \hat{L}_i \quad J_1, \cdots, J_2^n = \phi(1..n) \\
\end{array} \right) \) | \( S \leq_h \sum_{i \in J_k} T_i \Rightarrow A_k \) | \( \left( \begin{array}{l}
S \leq_h \sum_{i \in J_k} T_i \Rightarrow A_k \\
\text{or} \\
S' \leq_h \sum_{i \in 1..n \setminus J_k} T_i' \Rightarrow A_k \\
\end{array} \right) \) |
| \( L[S], S' \leq_h T \Rightarrow A_{2^n} \) | \( S, S'' \leq_h T \Rightarrow A' \) | \( S', S'' \leq_h T \Rightarrow A'' \) |
| (union) | \( S', S'' \leq_h T \Rightarrow A' \) | \( S, S'' \leq_h T \Rightarrow A'' \) |
| \( S, S'' \leq_h T \Rightarrow A' \) | \( S', S'' \leq_h T \Rightarrow A'' \) | \( (S, T) \in A \) |
| (star) | \( \mathcal{E}(U), S \leq_h T \Rightarrow A'' \) | \( \langle \mathcal{E}(U), S \rangle, S' \leq_h T \Rightarrow A'' \) |
| \( U, S \leq_h T \Rightarrow A'' \) | \( S', S'' \leq_h T \Rightarrow A'' \) | \( S \leq_h T \Rightarrow A \) |

2, 3, 4.a and 4.b of \(<\); respectively. The remaining rules are used for reducing the computation to such rules. Rule (union) applies to schemas \( S + S', R \) and verifies that both \( S, R \) and \( S', R \) are subschemas of \( T \). Rule (name) accounts for left schemas of shape \( U, S \). In this case the name \( U \) is replaced by its definition \( \mathcal{E}(U) \), the set of assumptions is extended with the pair \( (U, S, T) \) and the relation \( \leq \) is computed on these new arguments. Rule (star) is similar to (name) but for starred schemas. Rule (asmp) terminates proofs when the arguments are already in the set of assumptions.

The relation \( \leq \) is sound with respect to \(<\).

**Lemma 15 (Soundness)** If \( S \leq_h T \Rightarrow A \), then \( S <: T \).
Proof: Let $\mathcal{R}$ be the relation containing

1. pairs $(S', T')$ such that a subtree $S' \preceq \mathcal{R} T'$ exists in the tree $S \preceq \emptyset T \Rightarrow \mathcal{A}$;
2. if $(B, T') \in \mathcal{R}$, then $(B, \emptyset, T') \in \mathcal{R}$, too. Similarly for pairs $((S')^*, T')$, $(\langle S'\rangle^*, T')$, $(L[S'], T')$, $(S' + S'', T')$, $(\emptyset, T')$, and $(S^*, T')$.

To check that $\mathcal{R}$ is a subschema relation, let $(S', T') \in \mathcal{R}$ and $S' \downarrow R$. By induction on the structure of the proof $S' \downarrow R$ it is easy to show that $(R, T) \in \mathcal{R}$, too. □

We note that the rules in Table C.1 define a program, which we call the $\preceq$-program, that takes a triple $(S, T, \mathcal{A})$ and attempts to build the proof tree by recursively analyzing the structure of $S$ and the set $\mathcal{A}$. The program returns a set $\mathcal{A}'$ if the attempt succeeds, returns a failure otherwise. The $\preceq$-program terminates. To demonstrate this property we introduce some notation:

- $t(S)$, called the set of subterms of $S$, is the smallest set satisfying the equations:
  
  $t(\emptyset) = \{ \}$
  $t(B) = \{ B \} \cup \{ B, \emptyset \}$
  $t(U) = \{ U \} \cup \{ U, \emptyset \} \cup \{ t(E(U)) \}$
  $t((S)^*) = \{ (S)^* \} \cup \{ (S)^*, \emptyset \} \cup \{ t(S) \}$
  $t(L[S]) = \{ L[S] \} \cup \{ L[S], \emptyset \} \cup \{ t(S) \}$
  $t(S, S') = \{ T, S' \mid T \in t(S) \} \cup \{ t(S') \}$
  $t(S^*) = t(S) \cup \{ S^* \} \cup \{ S, S^* \} \cup \{ \emptyset \}$
  $t(S + T) = \{ S + T \} \cup t(S) \cup t(T)$

- It is easy to demonstrate that $t(S)$ is always finite.
  - $\text{anames}(S)$ is the set $\{ U, T : U, T \in t(S) \} \cup \{ T^*, T^* : T^* \in t(S) \}$
  - $\text{lsubt}(S, T)$ is the smallest set containing $t(S)$, $t(T)$ and closed under the following properties:
    - if $L[Q], Q' \in \text{lsubt}(S, T)$ and $L'[Q''], Q'' \in \text{lsubt}(S, T)$ and $\hat{L} \not\subseteq \hat{L}'$ then
      $(L \setminus L')[Q], Q' \in \text{lsubt}(S, T)$ and $(L \cap L')[Q], Q' \in \text{lsubt}(S, T)$
    - if $S, S' \in t(S)$ and $T, T' \in t(S)$ then $S' + T' \in t(S)$.
    - Since $t(S)$ and $t(T)$ are finite then $\text{lsubt}(S, T)$ is finite as well.
  - $\| S \|_X$, called the size of $S$ with names in $X$, is the function inductively defined as:

$$
\| S \|_X = \begin{cases} 
0 & \text{if } S = U \in X \\
1 & \text{if } S = \emptyset \\
\| E(U) \|_{X \cup \{U\}} & \text{if } S = U \notin X \\
1 + \| T \|_X & \text{if } S = (T)^* \text{ or } S = L[T] \text{ or } S = T^* \\
1 + \| T \|_X + \| T' \|_X & \text{if } S = T, T' \text{ or } S = T + T'
\end{cases}
$$

The number $\| S \|_\emptyset$ is shortened into $\| S \|$.
We note that \(\|S\|\) and \(|t(S)|\) are finite (because \(E\) is a finite map). They are also different values in general. For instance \(\|S + S\| = 2 \times \|S\| + 1\) whilst \(|t(S + S)| = |t(S)| + 1\).

**Lemma 16** (1) The set \(\text{handles}(S)\) is always finite.

(2) The \(\preceq\)-program always terminates.

**Proof:** As regards (1), let \(h(S)\) be the function defined as

\[
h(S) = \begin{cases} 
0 & \text{if } S \text{ is empty} \\
1 & \text{if } S = () \text{ or } S = \langle T\rangle^c \\
1 & \text{if } S = L[T] \text{ and } S \text{ is not-empty} \\
h(T) + h(T') & \text{if } (S = T + T' \text{ or } S = T, T') \text{ and } S \text{ is not-empty} \\
1 + h(T) & \text{if } S = T^* \\
1 + h(E(U)) & \text{if } S \text{ is not-empty and } S = U
\end{cases}
\]

Since \(E\) is well-formed, \(h(S)\) is finite for every schema. The proof proceeds by induction on \(h(S)\). The base case is obvious. The inductive case is by cases on the structure of \(S\). We discuss the subcase \(S = U\). We observe that, by definition, \(\text{handles}(U) = \text{handles}(E(U))\). By inductive hypothesis \(\text{handles}(E(U))\) is finite; therefore \(\text{handles}(U)\) is finite as well.

As regards (2), let \(n_{S,T,A} = \|\text{anames}(S) \cup \text{anames}(T)\| \times \|\text{lsubt}(S,T)\| \setminus A\|\) (the subtrees of \(T\) are considered because of the contravariance of \(\langle \cdot \rangle^0\)). We note that \(A\) is contained into \((\text{anames}(S) \cup \text{anames}(T)) \times \|\text{lsubt}(S,T)\| \setminus A\|\). We demonstrate that every invocation of \(S \preceq_A T \Rightarrow A'\) in the premises of the rules of Table C.1 decreases the value \((n_{S,T,A}, \|S\| + \|T\|)\) (the order is lexicographic) of the conclusion. There is one problematic case: when the \(\preceq\)-program tries to apply (\text{split}). In this case, the value \((n_{S,T,A}, \|S\| + \|T\|)\) for the two premises is equal to that of the conclusion. However, after a finite number of application of (\text{split}) – corresponding (in the worst case) to the number of labelled handles of \(T\), which are finite by (1) – (\text{split}) reduces to (\text{lseq}). In (\text{lseq}) the value \((n_{S,T,A}, \|S\| + \|T\|)\) decreases, thus guaranteeing termination.

Completeness of \(\preceq\) with respect to \(\prec\): is demonstrated below.

**Definition 17** A triple \((S,T,A)\) is correct if and only if: (1) \(S \prec T\) and (2) \((S', T') \in A\) implies \(S' \prec T'\).

**Proposition 18** If \((S,T,A)\) is correct, then one of the rules in Table C.1 is applied by the \(\preceq\)-program and every judgment used in the premise of the rule is correct as well.

**Proof:** Together with the statement of the Proposition, we also demonstrate that if the \(\preceq\)-program returns a set \(A'\), then \(A'\) is correct: \((S', T') \in A'\) implies \(S' \prec T'\). We focus on not empty schemas \(S\) and the argument is by induction
on the structure of $S$. The case of empty schemas is immediate. The case $S = \emptyset$ is immediate as well. As inductive cases, we omit those where $S$ is a sequence of length 1 because they may be reduced to the following ones by Proposition 2(6). If $S = B_1, S'$, then, by $S <: T$, there exist $(T \downarrow B_i, T_i)_{i \in 1..n}$ such that, for every $i$, $B \subseteq B_i$ and $S' <: \sum_{i \in 1..n} T_i$. Therefore, the $\leq$-program may apply (BASE) reducing to the triple $(S', \sum_{i \in 1..n} T_i, A)$. The correctness of this triple follows by the hypotheses. The output set of the program is correct by inductive hypothesis. The case when $S = (S')^*, S''$ is similar to the previous one. When $S = L[S'], S''$ the $\leq$-program may apply (SPLIT) or (LSEQ) according to condition 4.a or 4.b of Definition 1 is used in $\leq$. Again, the correctness of every triple used in the premises follows by the hypotheses; the output set of every invocation of the program is correct by inductive hypothesis. If $S = S' + S'', R$ then, by Proposition 2(8), both $S', R <: T$ and $S'', R <: T$. Then the $\leq$-program may apply (UNION), thus reducing to two triples that are still correct. Similarly, the set that are returned by every invocation of the program are correct by inductive hypothesis. If either $S = U, S'$ or $S = S'^*, S''$ then the $\leq$-program may apply either (NAME) or (STAR) or (ASMP). In the first two cases, the correctness of the new triple follows by the correctness of the current triple. In the third case no new triple is generated. \[\square\]

Completeness is an immediate consequence of Proposition 18 and Lemma 16.

**Lemma 19 (Completeness)** If $S <: T$ then there exists $A$ such that $S \leq_\emptyset T \Rightarrow A$.

Rule (LSEQ) in Table C.1 retains a number of subtrees which is exponential in the size of the right schema. This causes an exponential cost for the $\leq$-program. Such a cost is an issue in Web-services, where data coming from untrusted parties, such as WSDL documents (containing the schema of a service), might be validated at run-time before processing. Since Web-services documents carry references, validation has to verify that the schema of the reference conforms with some expected schema, thus reducing itself to the subschema relation. It is worth to notice that in XDuce run-time subschema checks are avoided because programs are strictly coupled and typechecking guarantees that invalid values cannot be produced. In CDuce there is the possibility of using pattern matching on function values, thus invoking the subschema relation at run-time. However this feature is never used in CDuce programs.

In [11] a schema language restriction has been studied so that the corresponding subschema relation has a polynomial cost. Specifically, following XML-Schema, schemas are constrained in order to retain a deterministic model as regards tag-labelled transitions. The model is still nondeterministic with respect to channel-labelled transitions.
Definition 20  The set \( \text{l} \text{d} \text{e} \text{t} \) of label-determined schemas is the greatest set of schemas such that:

\[
\begin{align*}
() & \in \text{l} \text{d} \text{e} \text{t} \\
B & \in \text{l} \text{d} \text{e} \text{t} \\
\langle S\rangle^\kappa & \in \text{l} \text{d} \text{e} \text{t} \quad \text{if } S \in \text{l} \text{d} \text{e} \text{t} \\
L[S] & \in \text{l} \text{d} \text{e} \text{t} \quad \text{if } S \in \text{l} \text{d} \text{e} \text{t} \\
S, T & \in \text{l} \text{d} \text{e} \text{t} \quad \text{if } S \in \text{l} \text{d} \text{e} \text{t} \text{ and } T \in \text{l} \text{d} \text{e} \text{t} \\
S^* & \in \text{l} \text{d} \text{e} \text{t} \quad \text{if } S \in \text{l} \text{d} \text{e} \text{t} \\
S + T & \in \text{l} \text{d} \text{e} \text{t} \quad \text{if } S \downarrow L[S'], S'' \text{ and } T \downarrow L'[T'], T''' \text{ implies } \hat{L} \cap \hat{L}' = \emptyset \\
\text{and } S \in \text{l} \text{d} \text{e} \text{t}, T \in \text{l} \text{d} \text{e} \text{t} \\
U & \in \text{l} \text{d} \text{e} \text{t} \quad \text{if } \mathcal{E}(U) \in \text{l} \text{d} \text{e} \text{t} 
\end{align*}
\]

By the definition \( a[S] + (\sim a)[T] \) and \( \sim[S] + \langle S\rangle^\kappa + \langle T\rangle^\kappa' \) are label-determined schemas whilst \( a[ ] + (a + b)[ ] \) and \( \langle a[ ] + \sim[ ]\rangle^\kappa \) are not label-determined. It is worth to remark that every empty schema – the schema that does not retain any handle – is in \( \text{l} \text{d} \text{e} \text{t} \) and that schemas like \( a[ ] + a[\text{Empty}] \) are also label-determined.

We observe that, if \( S \) and \( T \) are label-determined then the proof of \( S \preceq_T A \) never requires the rule \((\text{lseq})\), which was problematic for its computational cost. Actually, in [11], the \( \preceq \)-program has been proved to have a polynomial cost when invoked on label-determined schemas.