LIF

Laboratoire d'Informatique Fondamentale
de Marseille

Unité Mixte de Recherche 6166
CNRS – Université de Provence – Université de la Méditerranée

A Typed Calculus for Querying Distributed XML Documents

Lucia Acciai, Michele Boreale and Silvano Dal Zilio

Rapport/Report 29-2006

October 2005

A Typed Calculus for Querying Distributed XML Documents

Lucia Acciai, Michele Boreale and Silvano Dal Zilio

LIF – Laboratoire d'Informatique Fondamentale de Marseille
UMR 6166
CNRS – Université de Provence – Université de la Méditerranée

dalzilio@lif.univ-mrs.fr

Abstract/Résumé

We study the problems related to querying large, distributed XML documents. Our proposal takes the form of a new process calculus in which XML data are processes that can be queried by means of concurrent pattern-matching expressions. What we achieve is a functional, strongly-typed programming model based on three main ingredients: an asynchronous process calculus that draws features from π-calculus and concurrent-ML; a model where both documents and expressions are represented as processes, and where evaluation is represented as a parallel composition of the two; a static type system based on regular expression types.

Keywords: Process calculi; XML; types.

Ce rapport s'intéresse aux problèmes liés à la manipulation et à l'interrogation de documents XML de très grande taille, distribués sur un réseau. Nous proposons un nouveau calcul de processus dans lequel les données sont des processus qui peuvent être interrogés par le biais d'expressions de filtrage concurrentes. Un des résultats de ce travail est un modèle de programmation fonctionnel, fortement typé, basé sur trois ingrédients principaux: un calcul de processus asynchrone qui emprunte certaines de ses caractéristiques au π-calcul et au langage CONCURRENT-ML; un modèle dans lequel documents et requêtes sont représentés par des processus et où l'évaluation d'une requête est représentée par la composition parallèle de ces deux processus; un système de typage statique basé sur les expressions régulières de types.

Mots-clefs: Calcul de processus; XML; types.

Relecteurs/Reviewers: Denis Lugiez and Solange Coupet-Grimal

Notes: This work was partly supported by ACI Masses de Données, project TRALALA.

1 Introduction

There is by now little doubt that XML will succeed as a lingua franca of data interchange on the Web. As a matter of fact, XML is a building block in the development of new models of concurrent applications, often referred to as Service-Oriented Architecture (SOA), where computational resources are made available on a network as a set of loosely-coupled, independent services.

The SOA model is characterized by the need to exchange and query XML documents. In this paper, we concentrate on the specific problems related to querying *large, distributed XML documents*. This is the case, for example, of applications interacting with distributed heterogeneous databases or that process data acquired dynamically, such as those originating from arrays of sensors (in this case, we can assume that the document is in effect infinite). For another example, consider the programs involved in the maintenance of the big Web indexes used by search engines [14]. A typical example is the computation of a *term vector*, that is a list of words found on some documents of the index together with their frequency. Distribution, concurrency and dynamic acquisition of data must be explicitly taken into account when designing an effective computational model for this kind of applications.

We most particularly pay attention to the processing model. Our proposal takes the form of a process calculus in which XML data are processes that can be queried by means of concurrent pattern-matching expressions. In this model, the evaluation of patterns is distributed among locations, in the sense that the evaluation of a pattern at a node triggers concurrent evaluation of sub-patterns at other nodes, and actions can be carried out upon success or failure of patterns. The calculus also provides primitives for storing and aggregating the results of intermediate computations and for orchestrating the evaluation of patterns. In this respect, we radically depart from previous works on XML-centered process calculi, see e.g. [2, 9, 17], where queries would be programmed as operations invoked on (servers hosting) Web Services and XML documents would be exchanged in messages. In contrast, we view queries as code being dispatched to the locations "hosting" a document. This shift of view is motivated by our target application domain. In particular, our model is partly inspired by the *MapReduce* paradigm described in [14] that is used to write programs to be executed on Google's large clusters of computers in a simple functional style. Continuing with the "term vector example" above, assume that the documents of interest are cached on different (maybe replicated) servers. A query that accomplishes the aforementioned task would dispatch sub-queries to every server and create a dedicated reference cell to aggregate the partial results from each server. Sub-queries sifts the local documents and transmit to the central reference cell a sequence of pairs (*word*, *frequency*) produced locally. The task of the aggregating function is to collect the frequencies for identical keywords as they arrive, so as to eventually produce the global term vector. To achieve reliability, sub-queries may have to report back periodically with status updates while the "master query" may decide to abort or reinstate queries in case of servers failure.

Another important feature of our model is the definition of a static type system based on *regular expression types* that is compatible with Document Type Definitions (DTD) and other XML schema languages. What we achieve is a functional, strongly-typed programming model for computing over distributed XML documents based on three main ingredients: a semantics defined by an asynchronous process calculus in the style of the π-calculus [23] and proposed semantics for concurrent-ML [16]; a model where documents and expressions are both represented as processes, and where evaluation is represented as a parallel composition of the two; a type system based on regular expression types (the soundness of the static semantics is proved via a subject reduction property, Theorem 1). Each of these choices is motivated by a feature of the problem: the study of service-oriented applications calls for including concurrency and explicit locations; the need to manipulate large, possibly dynamically generated, documents calls for a streamed model of processing; the documents handled by a service should often obey a predefined schema, hence the need to check that queries are well-typed, preferably before they are executed or "shipped".

The rest of the paper is organized as follows. Section 2 presents the core components of the calculus — documents, types and patterns — and Section 3 gives the formal semantics of the calculus. In Section 4 we define a first-order type system with subtyping based on regular expression types and prove the soundness of our type discipline. Before concluding with a review of related works, we study possible extensions of our model in Section 5.

2 Documents, Types and Patterns

We consider a simple language of first-order functional expressions, denoted $e, e', \ldots$, enriched with references and recursive pattern definitions that are used to extract values from documents. Patterns are built on top of a syntax for defining regular tree grammars [13], which is also at the basis of our type system.

2.1 Documents

An XML document may be seen as a simple textual representation for nested sequences of elements `<a>...</a>`. In this paper, we follow notations similar to [21] and choose a simplified version of documents by leaving aside attributes among other things. We assume an infinite set of *tag names*, ranged over by $\mathtt{a}, \mathtt{b}, \ldots$ (we will often choose the symbol $\boldsymbol{o}$ for the tag of the root element of a document). A document is an ordered sequence of elements $\mathtt{a_1}[v_1] \ldots \mathtt{a_n}[v_n]$, where $v_1, \ldots, v_n$ are documents. Documents may be empty, denoted `()`, and can be concatenated, denoted $v\mathbf{,}\, v'$. The composition operation is associative with identity `()`.

In the following we consider distributed documents, meaning that each element $\mathtt{a_j}[v_j]$ is placed in a given location, say $\imath_j$. Locations are visible only at the level of the operational semantics, in which the contents of a document is represented by the index $\imath_1 \ldots \imath_n$ (the list of locations) of its elements. For the sake of simplicity, locations and indexes are the only values handled in our calculus and we leave aside atomic data values such as strings or integers.

2.2 Document Types

Applications that exchange and process XML documents rely on type information, such as DTDs, to describe structural constraints on the occurrences of elements. In our model, types take the form of regular tree expressions, which are a set of recursive definitions of the form $A := \mathit{Reg}(\mathtt{a_i}[A_i])_{i \in 1..n}$, where Reg is a regular expression and $A, A_1, \ldots, A_n$ are type variables. This is essentially a syntax for defining regular tree grammar. A regular expression $\mathit{Reg}(\alpha_i)_{i \in 1..n}$ can be an atom α_i with $i \in 1..n$; it can be the constant `All`, which matches everything, or `Empty`, which matches the empty sequence; it can be a choice $\mathit{Reg}_1 \mid \mathit{Reg}_2$, a sequential composition $\mathit{Reg}_1, \mathit{Reg}_2$, or an iteration $\mathit{Reg}{*}$. For instance, the declaration below defines the type L of family trees, which are sequences of male or female person such that each person has a `name` element, and two elements, `d` and `s`, for the list of his daughters and sons.

$$\begin{array}{lcllcl} L & := & (\mathtt{man}[P] \,|\, \mathtt{woman}[P]){*} & P & := & \mathtt{name}[\mathtt{All}], \mathtt{d}[\mathit{WL}], \mathtt{s}[\mathit{ML}] \\ \mathit{WL} & := & \mathtt{woman}[P]{*} & \mathit{ML} & := & \mathtt{man}[P]\,{*}\,. \end{array}$$

There is a natural notion of subtyping $A <: B$ between regular expression types, meaning that every document in A is also in B. The type system is close to what is defined in functional languages for manipulating XML, see e.g. XDuce [19, 20, 21] or the review in [10], hence we stay consistent with actual frameworks used in sequential languages for processing XML data.

2.3 Selectors and Patterns

The core of our programming model is a system of distributed pattern matching expressions that concurrently sift through documents to extract information. Basically, patterns are types enhanced with parameters and capture variables. However, like functions, patterns are declared and have a name.

We assume a countable set of *names*, partitioned into *locations* $\imath, \jmath, \ell, \ldots$ and *variables* $x, y, \ldots$ We use the vector notation $\vec{x}$ for tuples of names. The declaration $p(\vec{x}) := \big(\mathit{Reg}(\mathtt{a_i}[p_i(\vec{y_i})])_{i \in 1..n}\big)$ `as` y defines a pattern called p, with parameters $\vec{x}$, that will collect matched documents in the reference y (where y is a variable in $\vec{x}$). For instance, the patterns defined below can be used to extract the names of persons occurring in a document of type L.

$$\begin{array}{rcl} \mathit{names}(x, y) & := & \big(\mathtt{man}[p(x, y, x)] \,|\, \mathtt{woman}[p(x, y, y)]\big){*} \\ p(x, y, z) & := & \mathtt{name}[\mathit{all}(z)], \mathtt{d}[\mathit{names}(x, y)], \mathtt{s}[\mathit{names}(x, y)] \\ \mathit{all}(z) & := & \mathtt{All\ as}\ z. \end{array}$$

A call to $\mathit{names}(\imath, \ell)$ stores in (the reference located at) $\imath$ the name of men and in ℓ the name of women. A call to $\mathit{names}(\ell, \ell)$ will store the names of all persons in ℓ. Actually, the most general form of pattern declaration allows `let` definitions and setting continuations to be evaluated upon success or failure of the pattern, i.e. a pattern declaration is of the form, where S is a selector $\mathit{Reg}(\mathtt{a_i}[p_i(\vec{y_i})])_{i \in 1..n}$:

$$p(\vec{x}) := \mathtt{let}\ \big(z_1 = e_1', \ldots, z_m = e_m'\big)\ \mathtt{in}\ \big(S\ \mathtt{as}\ y\big)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2\ \ ,$$

An important feature of our model is that patterns may extract multiple sets of values from documents in one pass, which contrasts with the monadic queries expressible with technologies such as XPath. In the next section, we give a formal definition of the calculus, which embeds an operator $\mathtt{try}\ v\ p(\vec{u})$ for applying the pattern p to the value v. During reduction, the index v is matched against S after all the expressions $e'_1, \ldots, e'_m$ have been evaluated. If the matching succeeds, then v is added to the values stored in y and e_1 is evaluated. Otherwise, the compensation e_2 is evaluated. These optional continuations allow to add basic exception and transaction mechanisms to the calculus.

Clearly, types are particular kind of patterns: a pattern declaration without parameters, `let` definitions, capture variables and continuations is a type declaration. Moreover, every pattern p can be associated with the type A obtained by erasing these extra information: A is the type of all documents that are matched by p.

In the following, we assume that functions and patterns are typed explicitly. For instance, we assume that the pattern $names$ is declared with the type $(\mathtt{All}, \mathtt{All}) \to L$. More generally, a reference that merges values of type B will have a type A such that $A, B <: A$.

2.4 Witness and Unambiguous Patterns

Next, we define what it means for a pattern to match an index and define a notion of *unambiguous* patterns. Assume S is the selector $\mathit{Reg}(\mathtt{a_i}[p_i(\vec{v_i})])_{i \in 1..m}$. The sequence $\mathtt{a_{i_1}} \ldots \mathtt{a_{i_n}}$ matches S if and only if it is a "word" in the language of $\mathit{Reg}(\mathtt{a_i})_{i \in 1..m}$. This relation is denoted $\mathtt{a_{i_1}} \ldots \mathtt{a_{i_n}} \vdash_S p_{i_1}(\vec{v}_{i_1}) \ldots p_{i_n}(\vec{v}_{i_n})$ and we call $(p_{i_j}(\vec{v}_{i_j}))_{j \in 1..n}$ a *witness* for S of $\mathtt{a_{i_1}} \ldots \mathtt{a_{i_n}}$. We write $\mathtt{a_{i_1}} \ldots \mathtt{a_{i_n}} \not\vdash_S$ if the sequence has no witness for S. More formally, the relation $\mathtt{a_1} \ldots \mathtt{a_n} \vdash_S c_1 \ldots c_n$, with $c_i ::= p(\vec{v}) \mid \mathtt{All}$, is defined in the following table:

Witness

(W-All)
$$\frac{}{\mathtt{a_1} \ldots \mathtt{a_n} \vdash_{\mathtt{All}} \mathtt{All} \ldots \mathtt{All}}$$

(W-Empty)
$$\frac{}{() \vdash_{\mathtt{Empty}} ()}$$

(W-Choice)
$$\frac{\exists i \in \{1, 2\} : \ \mathtt{a_1} \ldots \mathtt{a_n} \vdash_{\mathit{Reg}_i} c_1 \ldots c_n}{\mathtt{a_1} \ldots \mathtt{a_n} \vdash_{\mathit{Reg}_1 | \mathit{Reg}_2} c_1 \ldots c_n}$$

(W-Atom)
$$\frac{}{\mathtt{a} \vdash_{\mathtt{a}[c]} c}$$

(W-Seq)
$$\frac{\exists i \in \{0 \ldots n\} : \ \mathtt{a_1} \ldots \mathtt{a_i} \vdash_{\mathit{Reg}_1} c_1 \ldots c_i \quad \mathtt{a_{i+1}} \ldots \mathtt{a_n} \vdash_{\mathit{Reg}_2} c_{i+1} \ldots c_n}{\mathtt{a_1} \ldots \mathtt{a_n} \vdash_{\mathit{Reg}_1, \mathit{Reg}_2} c_1 \ldots c_n}$$

(W-Star-Empty)
$$\frac{}{() \vdash_{\mathit{Reg}*} ()}$$

(W-Star)
$$\frac{\exists i \in \{1 \ldots n\} : \ \mathtt{a_1} \ldots \mathtt{a_i} \vdash_{\mathit{Reg}} c_1 \ldots c_i \quad \mathtt{a_{i+1}} \ldots \mathtt{a_n} \vdash_{\mathit{Reg}*} c_{i+1} \ldots c_n}{\mathtt{a_1} \ldots \mathtt{a_n} \vdash_{\mathit{Reg}*} c_1 \ldots c_n}$$

It is standard in XML to restrict to expressions that denote sequences of elements unequivocally. We say that a pattern with selector S is *unambiguous* if each sequence of tags has at most one witness for S. Assume that $(p_{i_j}(\vec{v}_{i_j}))_{j \in 1..m}$ is "the witness" of S for $\mathtt{b_1} \ldots \mathtt{b_m}$. When a document $\mathtt{b_1}[v_1] \ldots \mathtt{b_m}[v_m]$ is matched against a pattern with selector S, each sub-document v_j is matched against $p_{i_j}(\vec{v}_{i_j})$. If $\mathtt{b_1} \ldots \mathtt{b_m}$ has no witness then the pattern-matching fails.

Some schema languages, like DTD for example [7], use a stronger notion which requires that the witness can be computed incrementally, reading from a sequence of tags with only one symbol look-ahead. While this notion is suitable when working with streamed data (of ordered documents) it may impose needless performance penalties when working in a truly concurrent way. For instance, we want to be able to start the evaluation on an element without necessarily matching all its preceding siblings beforehand (while still providing a minimal support for "set-at-a-time" operations). For this reason, we require an even stronger notion of unambiguity and say that a selector $Reg(\mathtt{a_i}[p_i(\vec{v_i})])_{i \in 1..n}$ is *consistently unambiguous* if every tag specifies a unique pattern, i.e. whenever $\mathtt{a_i} = \mathtt{a_j}$ then $p_i(\vec{v_i})$ and $p_j(\vec{v_j})$ are the same.

Another (more flexible but also more complex) solution would be to require that, for every sequence of tags and every integer i, the i^{th} component of a witness can be computed only from the value of the i^{th} tag.

3 The Calculus

The presentation of the calculus can be naturally divided into two fragments: a language of functional expressions, or *programs*, that are used in the body of pattern and function declarations; and a language of processes, or *configurations*, that models distributed documents and the concurrent execution of programs.

3.1 Programs

The calculus embeds a first-order functional language with references, pattern-matching and constructs for building documents. In the following, we assume that every function identifier f has associated arity $n \geqslant 0$ and a unique definition $f(\vec{x}) := e$ where the variables in $\vec{x}$ are distinct and include the free variables of e. We take similar hypotheses for patterns. The syntax of expressions $e, e', \ldots$ is given below:

Syntax of Expressions

$u, v ::=$	results
$\quad x$	$\quad$ name: variable or location
$\quad \imath_1 \ldots \imath_n$	$\quad$ index (with $n \geqslant 0$)
$e ::=$	expressions
$\quad u$	$\quad$ result
$\quad a[u]$	$\quad$ element creation
$\quad u\mathbf{,}\, v$	$\quad$ result composition
$\quad f(u_1, \ldots, u_n)$	$\quad$ function call
$\quad \mathtt{let}\ x = e_1\ \mathtt{in}\ e_2$	$\quad$ let
$\quad \mathtt{newref}\ u$	$\quad$ new reference (with initial value u)
$\quad !u$	$\quad$ dereferencing

$u \mathrel{+}= v$	update (adds v to the values stored in u)
$\mathtt{try}\ u\ p(u_1, \ldots, u_n)$	pattern matching call
$\mathtt{wait}\ u(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$	wait matching

A result is either a name or an index, i.e. an expression that immediately returns itself. Expressions include results, operators for creating new elements $\mathtt{a}[u]$, for concatenating indexes u, v, and for creating and accessing references. Reference update has a slightly unusual semantics since the effect of $\imath \mathrel{+}= v$ is to append v to the value stored in the reference $\imath$. Actually, we could imagine that each reference is associated with an "aggregating function" that specifies how the sequence of values stored in the reference has to be combined. For example, assume ℓ is an "integer reference" that increments its value by one on every assignment. Then a call to $names(\ell, \ell)$ counts the number of people in a document of type L. We only consider index composition in this work.

The expression $\mathtt{try}\ v\ p(\vec{u})$ is used to apply the pattern p to the index $v = \imath_1 \ldots \imath_n$. A $\mathtt{try}$ expression returns at once with the location of a fresh node where the matching occurs. Moreover, evaluation of patterns is carried out concurrently: the effect of evaluating $\mathtt{let}\ z = \big(\mathtt{try}\ v\ p(\vec{u})\big)\ \mathtt{in}\ P$ is to filter v by p concurrently with the evaluation of P. In this example, z is bound to the location of the "thread" that executes the $\mathtt{try}$ expression, say ℓ. The location ℓ can be tested in P to check whether the pattern-matching has ended using the expression $\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$. The $\mathtt{wait}$ statement blocks until the pattern evaluating at ℓ stops. Then the continuation e_1 is evaluated if the matching succeeds, otherwise e_2 is evaluated. In each case the variable x is bound to v.

3.2 Configurations

The syntax of processes $P, Q, \ldots$ is as follows:

Syntax of Processes

$P, Q, R ::=$	processes
e	expression
$\mathtt{let}\ x = P\ \mathtt{in}\ Q$	let
$\langle\, \imath \mapsto d \,\rangle$	location
$P \upharpoonright Q$	parallel composition
$(\nu\imath)P$	restriction
$d ::=$	resources
$\mathtt{ref}\ u$	reference with value u
$\mathtt{node}\ \mathtt{a}(u)$	node, element tagged $\mathtt{a}$ with index u
$\mathtt{try}\ \imath\ p(u_1, \ldots, u_n)$	try matching
$\mathtt{test}\ \imath\ u$	test matching
$\mathtt{ok}\ \imath$	successful match
$\mathtt{fail}\ \imath$	failed match

The calculus features operators from the π-calculus: restriction $(\nu\imath)P$ specifies the scope of a name $\imath$ local to P; parallel composition $P \Rsh Q$ represents the concurrent evaluation of P and Q. Overall, a process is a multiset of `let` expressions, describing threads execution, and locations $\langle\, \imath \mapsto d \,\rangle$, that describes a *resource* d located in $\imath$.

The calculus is based on an abstract notion of location that is, at the same time, the minimal unit of interaction and the minimal unit of storage. Failures are not part of this model (they can be viewed as an orthogonal feature) but could be added, e.g. in the style of [5]. Locations store resources. The main resources are `ref` u, to store the current state of a reference, and `node a`(u), to describe an element of the form $\mathtt{a}[u]$. The calculus explicitly takes into account the distribution of document nodes and, for example, the document $\mathtt{a}[\mathtt{b}[\,]\ \mathtt{c}[\,]]$ can be represented (at runtime) by the parallel composition:

$$(\nu\imath_1\imath_2)\big(\langle\, \imath \mapsto \mathtt{node\ a}(\imath_1\ \imath_2) \,\rangle \Rsh \langle\, \imath_1 \mapsto \mathtt{node\ b}(\,) \,\rangle \Rsh \langle\, \imath_2 \mapsto \mathtt{node\ c}(\,) \,\rangle\big) \quad .$$

The other resources arise in the evaluation of pattern-matching and correspond to different phases in its execution: scheduling a "pattern call" (`try`); waiting for the result of sub-patterns (`test`); stopping and reporting success (`ok`) or failure (`fail`).

Syntactic conventions: the operators `let`, `wait` and ν are name binders. Notions of α-equivalence and of free and bound names arise as expected: we denote $fv(P)$ the set of variables that occur free in P and $fn(P)$ the set of free names. We identify expressions and terms up-to α-equivalence. Substitutions are finite partial maps from variables to results: we write $P\{x \leftarrow u\}$ for the simultaneous, capture-avoiding substitution of all free occurrences of x in P with u. Assume σ is the substitution $\{x_1 \leftarrow u_1\} \dots \{x_n \leftarrow u_n\}$ and $\vec{u} = (u_1, \dots, u_n)$. We write $f(\vec{u}) := e'$ if $f(\vec{x}) := e$ and $e' = \sigma(e)$ and we write $p(\vec{u}) := S'$ if the selector of $p(\vec{x})$ is S and $S' = \sigma(S)$. Finally, we make use of the following abbreviations: if $u = \imath_1 \dots \imath_n$ then $(\nu u)P$ is a shorthand for $(\nu\imath_1) \dots (\nu\imath_n)P$; the term $(\nu\ell)P \Rsh Q$ stands for $((\nu\ell)P) \Rsh Q$; the term $\mathtt{let}\ x = P\ \mathtt{in}\ Q \Rsh R$ stands for $(\mathtt{let}\ x = P\ \mathtt{in}\ Q) \Rsh R$; and $\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1$ stands for $\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ \mathtt{()}$ (and similarly for omitted `then` clause).

3.3 Reduction Semantics

The semantics of our calculus follows the chemical style found in the π-calculus [23]: it is based on structural congruence and a reduction relation. Reduction represents individual computation steps and is defined in terms of structural congruence and evaluation contexts.

Structural congruence $\equiv$ allows the rearrangement of terms so that reduction rules may be applied. It is the least congruence on processes to satisfy the following axioms:

Structural Congruence: $P \equiv Q$

(Struct Par Assoc)

$$\frac{}{(P \Rsh Q) \Rsh R \equiv P \Rsh (Q \Rsh R)}$$

(Struct Par Let)

$$\frac{x \notin fn(P)}{P \Rsh \mathtt{let}\ x = Q\ \mathtt{in}\ R \equiv \mathtt{let}\ x = (P \Rsh Q)\ \mathtt{in}\ R}$$

(Struct Par Com)

$$\frac{}{(P \Rsh Q) \Rsh R \equiv (Q \Rsh P) \Rsh R}$$

(Struct Res Let)

$$\frac{\ell \notin \mathit{fn}(Q)}{(\nu\ell)\texttt{let}\ x = P\ \texttt{in}\ Q \equiv \texttt{let}\ x = (\nu\ell)P\ \texttt{in}\ Q}$$

(Struct Res Res)

$$\frac{}{(\nu\imath)(\nu\ell)P \equiv (\nu\ell)(\nu\imath)P}$$

(Struct Res Par R)

$$\frac{\imath \notin \mathit{fn}(P)}{(\nu\imath)(P \Rsh Q) \equiv P \Rsh (\nu\imath)Q}$$

(Struct Res Par L)

$$\frac{\imath \notin \mathit{fn}(Q)}{(\nu\imath)(P \Rsh Q) \equiv ((\nu\imath)P) \Rsh Q}$$

(Struct Let Assoc)

$$\frac{x \notin \mathit{fn}(R)}{\texttt{let}\ y = (\texttt{let}\ x = P\ \texttt{in}\ Q)\ \texttt{in}\ R \equiv \texttt{let}\ x = P\ \texttt{in}\ (\texttt{let}\ y = Q\ \texttt{in}\ R)}$$

Since a process may return a value, we take the convention that the result of a composition $P_1 \Rsh \ldots \Rsh P_n$ is the result of its rightmost term P_n. The values returned by the other processes are discarded. This entails that the order of parallel components is relevant. For this reason, unlike the situation in most process calculi, parallel composition is not a commutative operator. Actually, composition is "left commutative", which means that $(P \Rsh Q) \Rsh R$ is equivalent to $(Q \Rsh P) \Rsh R$ but that we do not necessarily have $P \Rsh Q$ equivalent to $Q \Rsh P$. This choice is similar to what is found in calculi introduced for defining the semantics of concurrent-ML [16] and for concurrent extension of object calculi [18]. An advantage is that we directly include sequential composition of processes: the sequential composition $P; Q$ can be interpreted by the term $\texttt{let}\ x = P\ \texttt{in}\ Q$, where $x \notin \mathit{fv}(Q)$. Moreover it relieves us from the need to encode the operation of returning a result using continuations and sending a message on a result channel, as in the π-calculus.

Reduction $\rightarrow$ is the least binary relation on closed terms to satisfy the following rules.

Reduction: $P \rightarrow Q$

(Red Fun)

$$\frac{f \text{ declared as } f(\vec{x}) := e}{f(u_1, \ldots, u_n) \rightarrow e\{x_1 \leftarrow u_1\} \ldots \{x_n \leftarrow u_n\}}$$

(Red Let)

$$\frac{}{\texttt{let}\ x = u\ \texttt{in}\ P \rightarrow P\{x \leftarrow u\}}$$

(Red Struct)

$$\frac{P \equiv Q, \quad Q \rightarrow Q', \quad Q' \equiv P'}{P \rightarrow P'}$$

(Red Context)$^{(\star)}$

$$\frac{P \rightarrow P'}{E[P] \rightarrow E[P']}$$

(Red Ref)

$$\frac{u = \imath_1 \ldots \imath_n \quad \ell \text{ fresh name}}{\texttt{newref}\ u \rightarrow (\nu\ell)(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell)}$$

(Red Read)

$$\frac{}{\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh !\ell \rightarrow \langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh u}$$

(Red Write)$^{(\star\star)}$

$$\frac{w = u, v}{\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell \mathrel{+}= v \rightarrow \langle\, \ell \mapsto \texttt{ref}\ w \,\rangle \Rsh \texttt{()}}$$

(Red Node)

$$\frac{u = \imath_1 \ldots \imath_n \quad \imath \text{ fresh name}}{\mathtt{a}[u] \rightarrow (\nu\imath)(\langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(u)\,\rangle \Rsh \imath)}$$

(Red Comp)

$$\frac{u_1 = \imath_1 \ldots \imath_k \quad u_2 = \imath_{k+1} \ldots \imath_n}{u_1, u_2 \rightarrow \imath_1 \ldots \imath_n}$$

(Red Try)

$$\frac{u = \imath_1 \ldots \imath_n \qquad \imath, \ell \text{ distinct fresh names}}{\mathtt{try}\ u\ p(\vec{v}) \rightarrow (\nu\imath)(\nu\ell)(\langle\, \imath \mapsto \mathtt{node}\ \boldsymbol{o}(u)\,\rangle \Rsh \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v})\,\rangle \Rsh \ell\,)}$$

(Red Try Match)

$$\frac{\begin{array}{c} P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)\,\rangle \Rsh \prod_{k\in 1..n} \langle\, \imath_k \mapsto \mathtt{node}\ \mathtt{a}_k(w_k)\,\rangle \\ p(\vec{v}) := S \quad \mathtt{a}_1 \ldots \mathtt{a_n} \vdash_S p_1(\vec{v}_1) \ldots p_n(\vec{v}_n) \qquad w = \jmath_1 \ldots \jmath_n \text{ distinct fresh names} \end{array}}{P \Rsh \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v})\,\rangle \rightarrow P \Rsh (\nu w)\big(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \mathtt{try}\ \imath_k\ p_k(\vec{v_k})\,\rangle \Rsh \langle\, \ell \mapsto \mathtt{test}\ \imath\ w\,\rangle\big)}$$

(Red Try All)

$$\frac{}{\langle\, \ell \mapsto \mathtt{try}\ \imath\ \mathtt{All}\,\rangle \rightarrow \langle\, \ell \mapsto \mathtt{ok}\ \imath\,\rangle}$$

(Red Try Error)

$$\frac{\begin{array}{c} P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)\,\rangle \Rsh \prod_{k\in 1..n} \langle\, \imath_k \mapsto \mathtt{node}\ \mathtt{a}_k(w_k)\,\rangle \\ p(\vec{v}) := S \quad \mathtt{a}_1 \ldots \mathtt{a_n} \not\vdash_S \end{array}}{P \Rsh \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v})\,\rangle \rightarrow P \Rsh \langle\, \ell \mapsto \mathtt{fail}\ \imath\,\rangle}$$

(Red Try Error)

$$\frac{P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)\,\rangle \Rsh \prod_{k\in 1..n} \langle\, \imath_k \mapsto \mathtt{node}\ \mathtt{a}_k(w_k)\,\rangle \quad p(\vec{v}) := S \quad \mathtt{a}_1 \ldots \mathtt{a_n} \not\vdash_S}{P \Rsh \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v})\,\rangle \rightarrow P \Rsh \langle\, \ell \mapsto \mathtt{fail}\ \imath\,\rangle}$$

(Red Test Ok)

$$\frac{P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)\,\rangle \Rsh \prod_{k\in 1..n} \langle\, \jmath_k \mapsto \mathtt{ok}\ \imath_k\,\rangle \quad w = \jmath_1 \ldots \jmath_n}{P \Rsh \langle\, \ell \mapsto \mathtt{test}\ \imath\ w\,\rangle \rightarrow P \Rsh \langle\, \ell \mapsto \mathtt{ok}\ \imath\,\rangle}$$

(Red Test Fail)

$$\frac{\begin{array}{c} P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)\,\rangle \Rsh \prod_{k\in 1..n} \langle\, \jmath_k \mapsto d_k\,\rangle \qquad w = \jmath_1 \ldots \jmath_n \\ \forall k \in 1..n:\ d_k \in \{\mathtt{ok}\ \imath_k, \mathtt{fail}\ \imath_k\} \qquad \exists j \in 1..n:\ d_j = \mathtt{fail}\ \imath_j \end{array}}{P \Rsh \langle\, \ell \mapsto \mathtt{test}\ \imath\ w\,\rangle \rightarrow P \Rsh \langle\, \ell \mapsto \mathtt{fail}\ \imath\,\rangle}$$

(Red Wait Ok)

$$\frac{P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(u)\,\rangle \Rsh \langle\, \ell \mapsto \mathtt{ok}\ \imath\,\rangle}{P \Rsh \mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \rightarrow P \Rsh e_1\{x \leftarrow u\}}$$

(Red Wait Fail)

$$\frac{P = \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(u)\,\rangle \Rsh \langle\, \ell \mapsto \mathtt{fail}\ \imath\,\rangle}{P \Rsh \mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \rightarrow P \Rsh e_2\{x \leftarrow u\}}$$

$^{(\star)}$ where $E ::= Q \Rsh E \quad | \quad E \Rsh P \quad | \quad [.] \quad | \quad (\nu\ell)E \quad | \quad \mathtt{let}\ x = E\ \mathtt{in}\ P$

$^{(\star\star)}$ in the general case we have $w = \mathtt{op}(u, v)$, where op is some "aggregating" function

The rules for expressions are similar to traditional semantics for first-order languages, with the difference that the resources in a configuration play the role of the store. Likewise, the rules for operators that return new values (the operators `newref`, `a[]` and `try`) yields reductions of the form $e \rightarrow (\nu\ell)(\langle\, \ell \mapsto d \,\rangle \upharpoonright \ell)$, which means that new values are always allocated in a fresh location. Actually a quick inspection of the rules shows that resources are created in fresh locations and are always used in a linear way: an expression cannot discard a resource or create two different resources at the same location.

The remaining rules are related to the evaluation of pattern-matching expressions. A `try` expression on the pattern p generates a fresh `try` resource, rule (Red Try). Assume that S is the selector of p, the `try` resource will trigger evaluation of sub-patterns selected from a witness of S, rule (Red Try Match). For the sake of simplicity, we only consider selector patterns in rule (Red Try Match). In the general case, for patterns with local `let` definitions, capture variable and continuation, we can use the following rule:

$$\frac{\begin{array}{c} P \equiv \langle\, \imath \mapsto \texttt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n) \,\rangle \upharpoonright \prod_{k \in 1..n} \langle\, \imath_k \mapsto \texttt{node}\ \mathtt{a}_k(w_k) \,\rangle \\ p(\vec{v}) := \texttt{let}\ D\ \texttt{in}\ \big(S\ \texttt{as}\ v_k\big)\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \\ \mathtt{a_1} \ldots \mathtt{a_n} \vdash_S p_1(\vec{v_1}) \ldots p_n(\vec{v_n}) \qquad w = \jmath_1 \ldots \jmath_n \ \text{fresh names} \\ e_1' = \texttt{let}\ z = (v_k \mathrel{+}= (\imath_1 \ldots \imath_n))\ \texttt{in}\ e_1 \qquad z \ \text{fresh variable} \end{array}}{\begin{array}{l} P \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \quad \rightarrow \quad P \upharpoonright \big(\texttt{let}\ D\ \texttt{in}\ (\nu w)\big(\prod_{l \in 1..n} \langle\, \jmath_l \mapsto \texttt{try}\ \imath_l\ p_l(\vec{v_l}) \,\rangle \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ w\ e_1'\ e_2 \,\rangle\big)\big) \end{array}}$$

A `try` resource spawns new `try` resource and turns into a `test`, waiting for the results of these evaluations. Upon termination of all the sub-patterns, a `test` resource turns into `ok` or `fail`, rules (Red Test Ok) and (Red Test Fail). The `ok` and `fail` resources are immutable. The status of a pattern evaluation can be checked with the expression `wait` $\ell(x)$ `then` e_1 `else` e_2, see rules (Red Wait Ok) and (Red Wait Fail). If the resource at ℓ is `ok` $\imath$ then the `wait` expression evaluates to $e_1\{x{\leftarrow}v\}$, where v is the index of the node located at $\imath$. If the resource is `fail`$\imath$ then the expression evaluates to $e_2\{x{\leftarrow}v\}$. In all the other cases the expression is stalled.

Remark: in rule (Red Try Match), we compute the witness for all the children of an element in one go. This is not always realistic since the size of the children's index can be very large (actually, in real applications, big documents are generally shallow and have a large number of children). It is possible to refine the operational semantics so that each sub-pattern is fired separately, not necessarily following the order of the document, and we can imagine that indexes are implemented using streams or linked lists. We have chosen this presentation for sake of simplicity (it is one of the simplifications used in this paper so that we can concentrate on the innovative features of the calculus and its type system).

4 Static Semantics

The types of document indexes are the same than the types for documents defined in Section 2. Apart from regular expressions types A, the type t of a process can also be the resource type $\star$

(a constant type for terms that return no values); a reference type $\mathtt{ref}\ A$; a node type $\mathtt{node}\ \mathtt{a}(u)$ for the type of a location holding an element $\mathtt{a}[u]$; or a try type $\mathtt{loc}\ \mathtt{a}(A)$, that is the type of a location hosting the evaluation of a pattern of type A on the contents of an element tagged $\mathtt{a}$.

Types

$t ::=$	type
$\star$	no value
A	regular expression type
$\mathtt{ref}\ A$	reference
$\mathtt{node}\ \mathtt{a}(u)$	node location
$\mathtt{loc}\ \mathtt{a}(A)$	try location

We can easily adapt the definition of witness to types (a type is some sort of selector). Assume A is declared as $A := \mathit{Reg}(\mathtt{a_i}[A_i])_{i\in 1..n}$. We say that there is a witness for A of $\mathtt{a_{i_1}} \dots \mathtt{a_{i_m}}$, denoted $\mathtt{a_{i_1}} \dots \mathtt{a_{i_m}} \vdash_A A_{i_1} \dots A_{i_m}$, if and only if the sequence of tags $\mathtt{a_{i_1}} \dots \mathtt{a_{i_m}}$ is in the language of the regular expression $\mathit{Reg}(\mathtt{a_i})_{i\in 1..n}$. We can define the language of a type A as the set of documents that are matched by the pattern $\mathit{Reg}(\mathtt{a_i}[A_i])_{i\in 1..n}$. Based on this definition, we obtain a natural notion of subtyping $A <: B$, meaning that the language of A is included in the language of B. We write $A \doteq B$ if the languages of A and B are equal. We write $\overline{A}$ for some chosen regular expression type whose language is the complement of A. (The type $\overline{A}$ is unnecessary when $A \doteq \mathtt{All}$, which means that we do not need to introduce a type with an empty language.) In the case of type witness, we have $\mathtt{a_{i_1}} \dots \mathtt{a_{i_m}} \not\vdash_A$ if and only if there is a witness for $\overline{A}$ of $\mathtt{a_{i_1}} \dots \mathtt{a_{i_m}}$.

The type system is given in the following table. A type environment E is a finite mapping $x_1 : t_1, \dots, x_n : t_n$ between names and types. The type system is based on a single type judgment, $E \vdash P : t$, meaning that the process P has type t under the hypothesis E. We assume that there is a given, fixed set of type declarations of the form $A := \mathit{Reg}(\mathtt{a_i}[A_i])_{i\in 1..n}$. We assume that functions and patterns are well-typed, which is denoted $f : \vec{t} \to t_0$ and $p : \vec{t} \to A$. The types $t_1, \dots, t_n$ in $\vec{t}$ are the types of the parameters, while t_0 is the type of the body of f and A is the type of the selector of p. The type of a selector $S = \mathit{Reg}(\mathtt{a_i}[p_i(\vec{x_i})])_{i\in 1..n}$ is obtained from S by substituting to every pattern p_i in the selector its corresponding type A_i. Hence the type of S is equivalent to some type variable A such that $A := \mathit{Reg}(\mathtt{a_i}[A_i])_{i\in 1..n}$.

Typing Rules: $E \vdash P : t$

(Type x)
$$\frac{}{E, x : t, E' \vdash x : t}$$

(Type Sub)
$$\frac{A <: B \quad E \vdash P : A}{E \vdash P : B}$$

(Type Fun)
$$\frac{f : (t_1, \dots, t_n) \to t_0 \quad E \vdash u_i : t_i \quad i \in 1..n}{E \vdash f(\vec{u}) : t_0}$$

(Type Let)
$$\frac{E \vdash P : t \quad E, x{:}t \vdash Q : t'}{E \vdash \mathtt{let}\ x = P\ \mathtt{in}\ Q : t'}$$

(Type Doc)
$$\frac{E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(u_k) \quad E \vdash u_k : B_k \quad k \in 1..n}{E \vdash \imath_1 \dots \imath_n : \mathtt{a_1}[B_1], \dots, \mathtt{a_n}[B_n]}$$

(Type Node)
$$\frac{E \vdash u : A}{E \vdash \mathtt{a}[u] : \mathtt{a}[A]}$$

(Type Comp)
$$\frac{E \vdash u_i : A_i \quad i \in \{1,2\}}{E \vdash u_1, u_2 : A_1, A_2}$$

(Type Ref)
$$\frac{E \vdash u : A}{E \vdash \texttt{newref}\ u : \texttt{ref}\ A}$$

(Type Read)
$$\frac{E \vdash u : \texttt{ref}\ A}{E \vdash {!u} : A}$$

(Type Write)
$$\frac{E \vdash u : \texttt{ref}\ A \quad E \vdash v : B \quad A, B <: A}{E \vdash u \mathrel{+}= v : \texttt{Empty}}$$

(Type Res)
$$\frac{E, \ell_1 : t_1, \ldots, \ell_n : t_n \vdash P : t \qquad u = (\ell_1 \ldots \ell_n) \quad u \cap \mathit{fn}(E) = \emptyset}{E \vdash (\nu u)P : t}$$

(Type Par)
$$\frac{E \vdash P : t' \quad E \vdash Q : t}{E \vdash P \upharpoonright Q : t}$$

(Type Try Doc)
$$\frac{p : (t_1, \ldots, t_n) \to A \qquad E \vdash v_i : t_i \quad i \in 1..n \quad E \vdash u : B}{E \vdash \texttt{try}\ u\ p(v_1, \ldots, v_n) : \texttt{loc}\ \boldsymbol{o}(A)}$$

(Type Wait)
$$\frac{E \vdash u : \texttt{loc}\ \mathtt{a}(A) \qquad E, x : A \vdash e_1 : t \quad E, x : \overline{A} \vdash e_2 : t}{E \vdash \texttt{wait}\ u(x)\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t}$$

(Type Loc Ref)
$$\frac{E \vdash \ell : \texttt{ref}\ A \quad E \vdash u : A}{E \vdash \langle\, \ell \mapsto \texttt{ref}\ u \,\rangle : \star}$$

(Type Loc Node)
$$\frac{E \vdash \ell : \texttt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)}{E \vdash \langle\, \ell \mapsto \texttt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n) \,\rangle : \star}$$

(Type Loc Ok)
$$\frac{E \vdash \ell : \texttt{loc}\ \mathtt{a}(A) \quad E \vdash \imath : \texttt{node}\ \mathtt{a}(u) \qquad u = \imath_1 \ldots \imath_n \quad E \vdash u : A}{E \vdash \langle\, \ell \mapsto \texttt{ok}\ \imath \,\rangle : \star}$$

(Type Loc Fail)
$$\frac{E \vdash \ell : \texttt{loc}\ \mathtt{a}(A) \quad E \vdash \imath : \texttt{node}\ \mathtt{a}(u) \qquad u = \imath_1 \ldots \imath_n \quad E \vdash u : \overline{A}}{E \vdash \langle\, \ell \mapsto \texttt{fail}\ \imath \,\rangle : \star}$$

(Type Try Loc)
$$\frac{E \vdash \ell : \texttt{loc}\ \mathtt{a}(A) \quad E \vdash \imath : \texttt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n) \quad p : (t_1, \ldots, t_n) \to A \quad E \vdash v_i : t_i \quad i \in 1..n}{E \vdash \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle : \star}$$

(Type Test Loc)
$$\frac{E \vdash \ell : \texttt{loc}\ \mathtt{a}(A) \quad E \vdash \imath : \texttt{node}\ \mathtt{a}(u) \quad E \vdash \jmath_k : \texttt{loc}\ \mathtt{a}_\mathtt{k}(A_k) \qquad w = (\jmath_1 \ldots \jmath_n) \quad \mathtt{a}_1 \ldots \mathtt{a}_\mathtt{n} \vdash_A A_1 \ldots A_n}{E \vdash \langle\, \ell \mapsto \texttt{test}\ \imath\ w \,\rangle : \star}$$

The typing rules for the functional part of the calculus are standard. In what follows, we consider that references can only hold document values: a reference is of type $\texttt{ref}\ A$ and not $\texttt{ref}\ t$. Moreover, since a reference collects the sequence of values that are assigned to it, we check for every assignment of a value of type B into a reference of type $\texttt{ref}\ A$ that the relation $A, B <: A$ holds, see rule (Type Write). This check allows us to enforce statically the type of references.

The remaining typing rules are for resources and pattern-matching operators. The type of an expression $\texttt{try}\ u\ p(\vec{v})$ is $\texttt{loc}\ \boldsymbol{o}(A)$ if the pattern p matches documents of type A, see rule (Type Try Doc). Indeed the effect of this expression is to return a fresh location hosting the evaluation of p on an element of the form $\boldsymbol{o}[u]$. Correspondingly, a wait expression is well typed only if it is blocking on a location of type $\texttt{loc}\, a(A)$, that is the location of a resource that can eventually turn into `ok` or `fail`. The important aspect of this rule is that, while the continuations e_1 and e_2 of the `wait` expression must have the same type, they are typed under different typing environment: the expression e_1 is typed with the hypothesis $x : A$ while e_2 is typed with the hypothesis $x : \overline{A}$. This leads to more precise types for filtering expressions (see below).

The typing rules for locations are straightforward. Since a resource returns no value it has type $\star$. By rule (Type Try Loc), a location ℓ containing a `try` resource, evaluating a pattern p of type A, is well typed if ℓ is of type $\texttt{loc a}(A)$ and the root tag of the evaluated document is $\texttt{a}$. Note that no assumption is made on $(\imath_1, \ldots, \imath_n)$, which might well not be of type A. Finally, the rule for node location, (Type Loc Node), states that a location containing $\texttt{node a}(u)$ has only one possible type, namely $\texttt{node a}(u)$ itself. Hence this rule avoids the presence of two `node` resources with the same location but containing different elements. Actually, we could extend our type system in a simpler way to ensure that a well-typed configuration cannot have two resources at the same location: we say that the configuration is *well-formed* (for a formal definition see Appendix A).

An important feature of our calculus is that every pattern is strongly typed: its type is the regular expression obtained by erasing capture variables. Likewise we can type locations, expressions and processes using a combination of regular expression types and `ref` types. As it is often the case with typed languages, the first important property we need to prove is that well-typedness of processes is preserved by reduction.

Theorem 1 (subject reduction) *Suppose that P is well formed and contains only unambiguous patterns and t contains only unambiguous types. If $E \vdash P : t$ and $P \rightarrow Q$ then $E \vdash Q : t$.*

Proof. See Appendix B. □

The proof of Theorem 1 is by induction on the derivation of the relation $P \rightarrow Q$. The proof is quite involved since it is not possible to reason on a whole document at once: its content is scattered across distinct resource locations. This complexity reflects actual restrictions imposed when working with distributed documents, e.g. that they can never be checked locally.

We do not state a *progress theorem* in connection with Theorem 1. Indeed, there exists no notion of errors in our calculus (like e.g. the notion of "message not understood" in object-oriented languages) as it is perfectly acceptable for a pattern matching to fail or to get blocked on a `wait` statement. Nonetheless the subject reduction theorem is still useful. For instance, we can use it for optimizations purposes, like detecting that a specific matching will always fail.

Well-Formed Environments and Well-Typed Patterns. The typing judgment $E \vdash P : t$ defined in page 13 relies on several auxiliary judgments that we describe in this section. The first judgment is for stating that an environment is well-formed, $E \vdash \diamond$, that is essentially that no variable is declared more than once in an environment.

Good environments

(Env $\emptyset$) $\dfrac{}{\emptyset \vdash \diamond}$

(Env x) $\dfrac{E \vdash \diamond \quad x \notin dom(E)}{E, x{:}t \vdash \diamond}$

The remaining judgments are for defining well-typed pattern and function definitions. Indeed, we assume in the typing rules (Type Fun), (Type Try Doc) and (Type Try Loc) that function and pattern declarations are well typed, meaning that the functional type (globally) associated to function or pattern identifiers is correct with respect to their definitions.

Well-Typed Declarations

(Type Selector)

$$\frac{\begin{array}{c} S = Reg(a_i[p_i(\vec{x_i})])_{iin1..n} \quad E \vdash p_i(\vec{x_i}) : (\vec{t_i}) \to A_i \quad i = 1, \ldots, n \\ Reg(a_i[A_i])_{i \in 1..n} \doteq A \end{array}}{E \vdash S : A}$$

(Type Pat)

$$\frac{\begin{array}{c} p(x_1, \ldots, x_n) := \texttt{let}\ z_1 = e'_1, \ldots, z_m = e'_m\ \texttt{in}\ S\ \texttt{as}\ x_k\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \\ fn(p(\vec{x})) \cap dom(E) = \emptyset \quad E, x_1{:}t_1, \ldots, x_n{:}t_n \vdash e'_i : t'_i \quad i \in 1..m \\ E, x_1{:}t_1, \ldots, x_n{:}t_n, z_1{:}t'_1, \ldots, z_m{:}t'_m \vdash S : A \quad A \text{ compatible with } t_k \\ E, x_1{:}t_1, \ldots, x_n{:}t_n, z_1{:}t'_1, \ldots, z_m{:}t'_m \vdash e_1 : t_{e_1} \\ E, x_1{:}t_1, \ldots, x_n{:}t_n, z_1{:}t'_1, \ldots, z_m{:}t'_m \vdash e_2 : t_{e_2} \end{array}}{E \vdash p(x_1, \ldots, x_n) : (t_1, \ldots, t_n) \to A}$$

(Type Fun dec)

$$\frac{f := e \quad E, x_1 : t_1, \ldots, x_n : t_n \vdash e : t_0}{E \vdash f(x_1, \ldots, x_n) : (t_1, \ldots, t_n) \to t_0}$$

Rule (Type Selector) state that the type of a selector S is obtained from S by substituting every pattern identifier p_i with the corresponding type A_i. Rule (Type Pat) checks if the definition $p(x_1, \ldots, x_n) := \texttt{let}\ z_1 = e'_1, \ldots, z_m = e'_m\ \texttt{in}\ S\ \texttt{as}\ x_k\ \texttt{then}\ e_1\ \texttt{else}\ e_2$ respects the declared type $(t_1, \ldots, t_n) \to A$. Therefore, that upon receiving its actual parameters of type $t_1, \ldots, t_n$ and evaluating the expressions in the `let` part, pattern p actually matches documents of type A. In particular it is checked that the type of the selector S is A, that continuations e_1 and e_2 are well typed, and that the type t_k associated to the capture variable x_k is compatible with A, that is t_k is of the form `ref` B and $B, A <: B$. Rule (Type Fun dec) verifies if the definition $f := e$ complies with the type $(t_1, \ldots, t_n) \to t_0$ by checking if the type of the expression e is t_0 when evaluated in a context where the formal parameter of f have associated types $t_1, \ldots, t_n$.

5 Examples and Possible Extensions

We study examples that show how to interpret interesting programming idioms in our model, like spawning an expression in a new thread or handling user-defined exceptions.

5.1 Types and Pattern-Matching

We can encode a "traditional" `match` operator, as found in XDuce for example, that matches the pattern p against u and conditionally proceeds with e_1 or e_2. Assume y is a fresh variable ($y \notin fv(e_1) \cup fv(e_2)$), we define:

$$\texttt{match}\ u\ \texttt{with}\ p(\vec{v})\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \ =_{\text{def}} \left\{ \begin{array}{l} \texttt{let}\ x = \big(\texttt{try}\ u\ p(\vec{v})\big) \\ \ \texttt{in}\ \big(\texttt{wait}\ x(y)\ \texttt{then}\ e_1\ \texttt{else}\ e_2\big) \end{array} \right. \quad .$$

This example allows us to emphasize the role of the variable y when typing a `wait` statement. Let $e =_{\text{def}} \big(\texttt{match}\ z\ \texttt{with}\ \texttt{Empty}\ \texttt{then}\ \texttt{a}[z]\ \texttt{else}\ z\big)$ be the expression that returns z if it is not empty else returns $\texttt{a}[z]$. Assume z is a variable of type `All`, then the most precise type for e is also `All`. In contrast, if we consider the expression $\texttt{let}\ x = \big(\texttt{try}\ z\ \texttt{Empty}\big)\ \texttt{in}\ \big(\texttt{wait}\ x(y)\ \texttt{then}\ \texttt{a}[y]\ \texttt{else}\ y\big)$, which is equivalent to e, we obtain the more precise type $\overline{\texttt{Empty}}$, that is, we prove that the returned value cannot be empty. Indeed y plays the role of an alias for the value of z that is used with type `Empty` in the continuation $\texttt{a}[y]$ and with type $\overline{\texttt{Empty}}$ in y (and we have $\texttt{a}[\texttt{Empty}] <: \overline{\texttt{Empty}}$).

5.2 Concurrency

We show how to model simple threads, that is, we want to encode an operator `spawn` such that the effect of $\texttt{spawn}\ e_1;\ e_2$ is to evaluate e_1 in parallel with e_2, yielding the value of e_2 as a result. The simplest solution is to interpret $\texttt{spawn}\ e_1;\ e_2$ by the configuration $e_1 \upharpoonright e_2$. A disadvantage of this solution is that it is not possible to test in e_2 whether the evaluation of e_1 has ended.

Another simple approach to encode `spawn` is to rely on the pattern-matching mechanism. Let p be the pattern $p(\,) := (\texttt{Empty}\ \texttt{then}\ e_1)$. We can interpret the statement $\texttt{spawn}\ e_1; e_2$ with the expression $\texttt{let}\ x = (\texttt{try ()}\ p(\,))\ \texttt{in}\ e_2$. Indeed we have:

$$\begin{array}{rl} \texttt{let}\ x = (\texttt{try ()}\ p(\,))\ \texttt{in}\ e_2 \ \rightarrow^* & (\nu \imath \ell)\big(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(\,)\,\rangle \upharpoonright \\ & \big(\texttt{let}\ z = e_1\ \texttt{in}\ \langle\, \ell \mapsto \texttt{ok}\ \imath\,\rangle\big) \upharpoonright e_2\{x \leftarrow \ell\}\big) \quad . \end{array}$$

In the resulting process, e_1 and e_2 are evaluated concurrently and the resource $\langle\, \ell \mapsto \texttt{ok}\ \imath\,\rangle$ cannot interact with e_2 until the evaluation of e_1 ends (see rule (Struct Par Let) for example). Hence an occurrence of the expression $(\texttt{wait}\ x(y)\ \texttt{then}\ e)$ in e_2 acts as an operator blocking the execution of e until e_1 returns a value. We can in fact improve our encoding so that the result of e_1 is bound to z in e as follows:

$$\texttt{spawn}\ e_1;\ e_2 \ =_{\text{def}} \ (\nu \imath \ell) \left(\begin{array}{l} \texttt{let}\ z = e_1\ \texttt{in}\ \big(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(z)\,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{ok}\ \imath\,\rangle\big) \\ \upharpoonright e_2\{x \leftarrow \ell\} \end{array} \right) \quad .$$

It emerges from this example that a `try` location can be viewed as a *future*, that is a reference to the "future result" of an asynchronous computation. More generally, we can liken a process $(\langle\, \imath \mapsto \texttt{node a}(u)\,\rangle \Rsh \langle\, \ell \mapsto \texttt{ok}\ \imath\,\rangle)$ to an (asynchronous) output action $\ell!\langle \texttt{ok}, u\rangle$ as found in process calculi such as the π-calculus. Similarly, we can compare an expression $\texttt{wait}\ \ell(x)\ \texttt{then}\ e_1\ \texttt{else}\ e_2$ with a combination of input action and matching, $\ell?(x).\{\texttt{ok} \Rightarrow e_1 \mid \texttt{fail} \Rightarrow e_2\}$, with the following synchronization rules:

$$\begin{array}{lllll} \ell!\langle \texttt{ok}, u\rangle & \parallel\ \ell?(x).\{\texttt{ok} \Rightarrow e_1 \mid \texttt{fail} \Rightarrow e_2\} & \rightarrow & \ell!\langle \texttt{ok}, u\rangle & \parallel e_1\{x{\leftarrow}u\} \\ \ell!\langle \texttt{fail}, u\rangle & \parallel\ \ell?(x).\{\texttt{ok} \Rightarrow e_2 \mid \texttt{fail} \Rightarrow e_2\} & \rightarrow & \ell!\langle \texttt{ok}, u\rangle & \parallel e_2\{x{\leftarrow}u\} \end{array}$$

The main distinction with "traditional process calculi" is that we are in a situation where inputs are replicated. For this reason, we can have multiple `wait` operators synchronizing on the same location ℓ without the need for global consensus (or a lock) on the resource at ℓ. Nonetheless, since the calculus can express atomic reads and writes on a shared memory, it could be useful to rely on a standard mutual exclusion algorithm for accessing references. We could also interpret high-level primitives for mutexes directly in our calculus (see e.g. [18] for an example). Note also that there is no need for replication in our calculus since resources are persistent and recursive behaviors can be encoded using recursive function declarations.

5.3 Exceptions

We show how to model a simple exception mechanism in our calculus. Suppose we need to check that a document u of type L (the type of family trees) contains only women. This can be achieved using the pattern declarations $p(\,) := \texttt{woman}[q(\,)]*$ and $q(\,) := \texttt{name}[\texttt{All}], \texttt{d}[p(\,)], \texttt{s}[\texttt{Empty}]$ and a matching expression $\texttt{try}\ u\ p(\,)$. A drawback of this approach is that we need to wait for the completion of all sub-patterns to terminate before completing the computation, even if the matching trivially fails because we find an element tagged `man` early in the matching. A natural optimization is to use an explicit handling of failures, e.g. to add primitives to kill and "ping" (the location of) a `try` resource in the style of [5]. Another solution is to encode a basic mechanism for handling exceptions using the following derived operators, where $\imath_e$ is a default name associated to the location $\langle\, \imath_e \mapsto \texttt{node}\ \boldsymbol{o}(\,)\,\rangle$:

$$\begin{array}{rcll} \texttt{exception} & = & (\nu\ell)\ell & \text{creates a fresh (location) exception} \\ \texttt{throw}\ \ell & = & \langle\, \ell \mapsto \texttt{ok}\ \imath_e\,\rangle \Rsh \texttt{()} & \text{raises an exception at } \ell \\ \texttt{catch}\ \ell\ e & = & \texttt{wait}\ \ell(x)\ \texttt{then}\ e & \text{catches exception } \ell \text{ and runs } e\ \ (x \notin fv(e)) \end{array}$$

A simple example is to raise the exception at the end of a computation, like in the expression $\texttt{let}\ x = \texttt{exception}\ \texttt{in}\ \big((\ldots; \texttt{throw}\ x) \Rsh \texttt{catch}\ x\ e\big)$. If and when the `throw` expression is evaluated, we obtain a configuration of the form $(\nu l)\big(\ldots \Rsh \langle\, \ell \mapsto \texttt{ok}\ \imath_e\,\rangle \Rsh \texttt{wait}\ \ell(x)\ \texttt{then}\ e\big)$, which starts the execution of e. For instance, it is possible to raise the exception in the compensation part of a pattern declaration and to redefine the pattern p above in: $p(x) := \texttt{woman}[q(\,)]*\ \texttt{else}\ \texttt{throw}\ x$.

With our encoding, it is not possible to abort the execution of a whole "program block" using exceptions. Using a more involved encoding, e.g. based on CPS transforms, we could interpret this more general exception model.

6 Future and related work

We study a formal model for computing over large, perhaps dynamically generated, distributed XML documents. We define a typed process calculus and show that it supports a first-order type system with subtyping based on regular expression types, a system compatible with DTD and other schema languages for XML. Our work may be compared with recent proposals for integrating XML data into π-calculus. It can also be compared with proposals for filtering and querying XML streams (or so-called *XML pipelining* frameworks) for which there exists almost no formal foundations.

6.1 Related Work

There are a few works mixing XML with process calculi: Iota [6] is a concurrent XML scripting language with channel-based communications that relies on types to guarantee the well-formedness (not the validity) of documents; XPi [2] is a typed π-calculus extended with XML values in which documents are exchanged during communications; PiDuce [9] features asynchronous communications and code mobility and includes pattern matching expressions with built-in type checks. In all these proposals, documents are first class values exchanged in messages, which make these approaches inappropriate in the case of very large or dynamically generated data. At the opposite, we consider documents as special kind of processes that can be randomly accessed through the use of distributed indexes.

Works on querying XML streams can be roughly divided in two approaches. The first is to provide efficient single-pass evaluator, working with one query at a time (generally XPath queries) on multiple documents. The second approach, in relation to peer-to-peer and event-notification systems, is to filter XML streams by a large number of queries. We look more closely at some examples of such systems. SPEX, XSQ and XSM [8, 12, 22] are single-pass evaluators of XPath queries in which queries are compiled into networks of independent, deterministic pushdown transducers with buffers. The query language in XSM is severely restricted and only streams with non-recursive structure definitions can be processed (this is akin to non-recursive types in our framework). XFilter, YFilter and XTrie [4, 15, 11] follow the second approach. XFilter is a filtering system based on finite state machines (FSM). It uses one FSM per path query and an indexing mechanism to allow all FSMs to be executed simultaneously during the processing of a document. YFilter extends XFilter using a lazy NFA-based representation in which state transitions for simultaneous queries are precomputed (hence exploiting commonalities among path queries). Likewise, XTrie is based on decomposing tree patterns into collection of substrings and indexing them using a trie with the purpose to share the processing of "common sub-queries".

Our work follows the first approach with some differences (patterns extend XPath queries and `try`-statements apply one pattern to one document at a time). Most notably, we take a strongly typed approach and, instead of using XPath or XQuery, we extend the functional approach taken in e.g. XDuce and define distributed *regular expression pattern*. As a byproduct, we also provide a possible semantics for a concurrent extensions of languages based on XDuce. Nonetheless, since our operational semantics does not dictate how regular patterns should be implemented, we can take inspiration from these systems to implement efficient and scalable filtering primitives in our calculus. Conversely, we could use our calculus to give a formal semantics to these systems.

6.2 Future Work

The goal of this paper is not to define a new programming language. We rather try to provide formal tools for the study of concurrent computation models based on service composition and streamed XML data. However our calculus could be a basis for developing concurrent extensions of strongly typed languages for XML, such as XDuce. It could also be used to provide the semantics of systems in which XML documents contain active code that can be executed on distributed sites (i.e. processes and document text are mixed), like in the Active XML system for example [1]. To this end, it will be necessary to add an "`eval/quote`" mechanisms, as in LISP or multi-stage programming languages [24], and to fundamentally revise our static type checking approach.

Our work raises questions concerning observational equivalences that we intend to study in future work. Another avenue to investigate is the encoding of other concurrency related primitives, like channel-based synchronization and distributed transactions, or the possibility to dynamically update documents.

References

[1] Abiteboul S., Benjelloun O., Milo T., Manolescu I., Weber R.: Active XML: Peer-to-Peer Data and Web Services Integration. In *Proc. of VLDB*, 2002.

[2] Acciai L., Boreale M.: XPi: a typed process calculus for XML messaging. In *Proc. of FMOODS*, LNCS vol. 3535, Springer, 2005.

[3] Acciai L., Boreale M., Dal Zilio, S.: A Typed Calculus for Querying Distributed XML Documents. LIF Research Report xx, 2006.

[4] Altinel M., Franklin M.J.: Efficient filtering of XML documents for selective dissemination information. In *Proc. of the 26th VLDB Conference*, 2000.

[5] Amadio R.: An Asynchronous Model of Locality, Failure And Process Mobility. In *Proc. of COORDINATION*, LNCS vol. 1282, Springer, 1997.

[6] Bierman G., Sewell P.: Iota: A concurrent XML scripting language with applications to Home Area Networking. TR 577, Computer Lab., Cambridge, 2003.

[7] Brüggemann-Klein A., Wood D.: One-unambiguous regular languages. Information and Computation, 142(2), 1998.

[8] Bry F., Furche T., Olteanu D.: An efficient single-pass query evaluator for XML data structure. TR PMS-FB-2004-1, Computer Science Institute, Munich, 2004.

[9] Brown A., Laneve C., Meredith G.: PiDuce: a process calculus with native XML datatypes. In *Proc. of Workshop on Web Services and Formal Methods*, 2005.

[10] Castagna G.: Pattern and types for querying XML documents. In *Proc. of DBPL*, XSYM 2005 joint keynote talk, 2005.

[11] Chan C.Y., Felber P., Garofalakis M., Rastogi R.: Efficient filtering of XML documents with XPath expressions. The VLDB Journal 11, 2002.

[12] Chawathe S.S., Peng F.: XPath Queries on Streaming Data. In *Proc. of SIGMOD*, 2003.

[13] Comon H., Dauchet M., Jacquemard F., Tison S., Lugiez D., Tommasi M.: *Tree Automata on their application*. 1999. `http://www.grappa.univ-lille3.fr/tata/`

[14] Dean J., Ghemawat, S.:MapReduce: Simplified Data Processing on Large Cluster. In *Proc. of OSDI*, 2004.

[15] Diao Y., Fisher P., Franklin M.J.: Yfilter: efficient and scalable filtering of XML documents. In *Proc. of 18th ICDE*, IEEE, 2002.

[16] Ferreira W., Hennessy M., Jeffrey A.S.: A theory of weak bisimulation for core CML. J. Functional Programming 8(5), 1998.

[17] Gardner P., Maffeis S.: Modelling dynamic web data. Theor. Comput. Sci. 342(1) (2005).

[18] Gordon A.D., Hankin P.D.: A concurrent object calculus: reduction and typing. In *Proc. of HLCL*. Electr. Notes Theor. Comput. Sci. 16(3), 1998.

[19] Hosoya H., Vouillon J., Pierce B.J.: Regular expression types for XML. ACM Transactions on Programming Languages and Systems, 27(1), 2004.

[20] Hosoya H., Pierce B.J.: Regular expression pattern matching for XML. In *Proc. of POPL*, 2001.

[21] Hosoya H., Pierce B.J.: XDuce: A Statically Typed XML Processing Language. In *Proc. of ACM Transaction on Internet Technology*, 2003.

[22] Ludäscher B., Mukhopadhyay P., Papakonstantinou Y.: A Tranducer-Based XML Query Processor. In *Proc. of VLDB*, 2002.

[23] Milner R.: Communicating and Mobile Systems: The π-Calculus. CUP , 1999.

[24] Taha W., Sheard T.: MetaML and multi-stage programming with explicit annotations. Theor. Comput. Sci. 248(1-2), 2000.

A Well-formedness

A well-formed process is a configuration where every location is defined once. In the style of [18] we add simple linearity constraints to the type system to ensure well-formedness and we show some properties of well-formed terms.

Definition 1 (well formed configuration) *A configuration P is* well formed *if for every location ℓ it contains at most one definition $\langle\, \ell \mapsto d \,\rangle$.*

It is convenient to define the *domain* of a configuration P, $\mathtt{dom}(P)$, to be the set of the names of the free location definitions in P:

Domain of a configuration

$$
\begin{array}{lcl}
\mathtt{dom}(e) & \triangleq & \emptyset \\
\mathtt{dom}(\mathtt{let}\ x = P\ \mathtt{in}\ Q) & \triangleq & \mathtt{dom}(P) \cup \mathtt{dom}(Q) \\
\mathtt{dom}(\langle\, \ell \mapsto d \,\rangle) & \triangleq & \{\ell\} \\
\mathtt{dom}(P \Rsh Q) & \triangleq & \mathtt{dom}(P) \cup \mathtt{dom}(Q) \\
\mathtt{dom}((\nu\ell)P) & \triangleq & \mathtt{dom}(P) \setminus \{\ell\}
\end{array}
$$

The well-formed configurations are given by the judgement $P : \mathtt{wf}$ defined in the following table:

Well-Formed configurations

(WF-Exp)
$$\frac{}{e : \mathtt{wf}}$$

(WF-Let)
$$\frac{P : \mathtt{wf} \quad Q : \mathtt{wf} \quad \mathtt{dom}(P) \cap \mathtt{dom}(Q) = \emptyset}{\mathtt{let}\ x = P\ \mathtt{in}\ Q : \mathtt{wf}}$$

(WF-Resource)
$$\frac{}{\langle\, \ell \mapsto d \,\rangle : \mathtt{wf}}$$

(WF Par)
$$\frac{P : \mathtt{wf} \quad Q : \mathtt{wf} \quad \mathtt{dom}(P) \cap \mathtt{dom}(Q) = \emptyset}{P \Rsh Q : \mathtt{wf}}$$

(WF-Res)
$$\frac{P : \mathtt{wf} \quad \ell \in \mathtt{dom}(P)}{(\nu\ell)P : \mathtt{wf}}$$

In what follows we show that well-formedness is preserved by structural congruence and reductions.

Proposition 2 (well formed subject congruence) *If $P : \mathtt{wf}$ and $P \equiv Q$ then $Q : \mathtt{wf}$ and $\mathtt{dom}(P) = \mathtt{dom}(Q)$.*

Proof. By induction on structural congruence rules:

(Struct Par Assoc) if $(P_1 \Rsh P_2) \Rsh P_3 : \mathtt{wf}$ then, by (WF-Par), $P_1 \Rsh P_2 : \mathtt{wf}$, $P_3 : \mathtt{wf}$ and $\mathtt{dom}(P_1 \Rsh P_2) \cap \mathtt{dom}(P_3) = \emptyset$. Again by (WF-Par), $P_1 : \mathtt{wf}$, $P_2 : \mathtt{wf}$ and $\mathtt{dom}(P_1) \cap \mathtt{dom}(P_2) = \emptyset$. $\mathtt{dom}(P_2) \cap \mathtt{dom}(P_3) = \emptyset$, thus, by (WF-Par), $P_2 \Rsh P_3 : \mathtt{wf}$ and $\mathtt{dom}(P_2 \Rsh P_3) \cap \mathtt{dom}(P_1) = \emptyset$, thus $P_1 \Rsh (P_2 \Rsh P_3) : \mathtt{wf}$. $\mathtt{dom}((P_1 \Rsh P_2) \Rsh P_3) = \mathtt{dom}(P_1) \cup \mathtt{dom}(P_2) \cup \mathtt{dom}(P_3) = \mathtt{dom}((P_1 \Rsh P_2) \Rsh P_3)$;

(Struct Par Let) if $P_1 \upharpoonright \mathtt{let}\, x = P_2\, \mathtt{in}\ P_3 : \mathtt{wf}$ then by (WF-Par) $P_1 : \mathtt{wf}$, $\mathtt{let}\, x = P_2\, \mathtt{in}\ P_3 : \mathtt{wf}$ and $\mathtt{dom}(P_1) \cap \mathtt{dom}(\mathtt{let}\, x = P_2\ \mathtt{in}\ P_3) = \emptyset$. By (WF-Let) , $\mathtt{let}\, x = P_2\ \mathtt{in}\ P_3 : \mathtt{wf}$ implies $P_2 : \mathtt{wf}$, $P_3 : \mathtt{wf}$ and $\mathtt{dom}(P_2) \cap \mathtt{dom}(P_3) = \emptyset$. Thus $\mathtt{dom}(P_1) \cap \mathtt{dom}(P_2) = \emptyset$ and rule (WF-Par) imply $P_1 \upharpoonright P_2 : \mathtt{wf}$ and by (WF-Let) and $\mathtt{dom}(P_1 \upharpoonright P_2) \cap \mathtt{dom}(P_3) = \emptyset$ we have $\mathtt{let}\, x = P_1 \upharpoonright P_2\, \mathtt{in}\ P_3 : \mathtt{wf}$. $\mathtt{dom}(P_1 \upharpoonright \mathtt{let}\, x = P_2\, \mathtt{in}\ P_3) = \mathtt{dom}(P_1) \cup \mathtt{dom}(P_2) \cup \mathtt{dom}(P_3) = \mathtt{dom}(\mathtt{let}\ x = P_1 \upharpoonright P_2\ \mathtt{in}\ \ P_3)$;

(Struct Par Com) it is similar to the (Struct Par Assoc);

(Struct Res Let) by rule (WF-Res) $(\nu\ell)\mathtt{let}\ x = P_1\ \mathtt{in}\ \ P_2 : \mathtt{wf}$ implies $\ell \in \mathtt{dom}(\mathtt{let}\ x = P_1\ \mathtt{in}\ \ P_2)$ and $\mathtt{let}\ x = P_1\ \mathtt{in}\ \ P_2 : \mathtt{wf}$. By (WF-Let) $P_1 : \mathtt{wf}$, $P_2 : \mathtt{wf}$ and $\mathtt{dom}(P_1) \cap \mathtt{dom}(P_2) = \emptyset$. $\ell \in \mathtt{dom}(\mathtt{let}\ x = P_1\ \mathtt{in}\ \ P_2)$ and $\ell \notin fn(P_2)$ (thus $\ell \notin \mathtt{dom}(P_2)$) implies $\ell \in \mathtt{dom}(P_1)$, thus by (WF-Res) $(\nu\ell)P_1 : \mathtt{wf}$ and by (WF-Let) $\mathtt{let}\ x = (\nu\ell)P_1\ \mathtt{in}\ \ P_2 : \mathtt{wf}$. $\mathtt{dom}((\nu\ell)\mathtt{let}\ x = P_1\ \mathtt{in}\ \ P_2) = (\mathtt{dom}(P_1) \cup \mathtt{dom}(P_2)) \setminus \{\ell\} = \mathtt{dom}(\mathtt{let}\ x = (\nu\ell)P_1\ \mathtt{in}\ \ P_2)$;

(Struct Res Res) by (WF-Res) $(\nu\, \imath)(\nu\, \ell)R$ implies $R : \mathtt{wf}$ and $\imath, \ell \in \mathtt{dom}(R)$, and by (WF-Res) $(\nu\, \ell)(\nu\, \imath)R : \mathtt{wf}$. $\mathtt{dom}((\nu\, \imath)(\nu\, \ell)R) = \mathtt{dom}(R) \setminus \{\imath, \ell\} = \mathtt{dom}((\nu\, \ell)(\nu\, \imath)R)$;

(Struct Res Par R) (Struct Res Par L) by (WF-Res) $(\nu\ \ell)(P_1 \upharpoonright P_2) : \mathtt{wf}$ implies $P_1 \upharpoonright P_2 : \mathtt{wf}$ and $\ell \in \mathtt{dom}(P_1 \upharpoonright P_2)$. By (WF-Par) $P_1 : \mathtt{wf}$, $P_2 : \mathtt{wf}$ and $\mathtt{dom}(P_1) \cap \mathtt{dom}(P_2) = \emptyset$ and by (Struct Res Par R) $\ell \in \mathtt{dom}(P_2)$ (resp. (Struct Res Par L) implies $\ell \in \mathtt{dom}(P_1)$). By rule (WF-Res) $(\nu\ \ell)P_2 : \mathtt{wf}$ (resp. $(\nu\ \ell)P_1 : \mathtt{wf}$); so by rule (WF-Par) $P_1 \upharpoonright ((\nu\ \ell)P_2) : \mathtt{wf}$ (resp. $((\nu\ \ell)P_1) \upharpoonright P_2 : \mathtt{wf}$). $\mathtt{dom}((\nu\ \ell)(P_1 \upharpoonright P_2)) = (\mathtt{dom}(P_1) \cup \mathtt{dom}(P_2)) \setminus \{\ell\} = \mathtt{dom}(P_1 \upharpoonright ((\nu\ \ell)P_2))$ because $\ell \in \mathtt{dom}(P_2)$ and $\ell \notin \mathtt{dom}(P_1)$;

(Struct Let Assoc) by rule (WF-Let) $\mathtt{let}\ x = (\mathtt{let}\ y = P_1\ \mathtt{in}\ \ P_2)\ \mathtt{in}\ \ P_3 : \mathtt{wf}$ implies $\mathtt{let}\ y = P_1\ \mathtt{in}\ \ P_2 : \mathtt{wf}$, $P_3 : \mathtt{wf}$ and $\mathtt{dom}(\mathtt{let}\ y = P_1\ \mathtt{in}\ \ P_2) \cap \mathtt{dom}(P_3) = \emptyset$. Again, by rule (WF Let), $P_1 : \mathtt{wf}$, $P_2 : \mathtt{wf}$ and $\mathtt{dom}(P_1) \cap \mathtt{dom}(P_2) : \mathtt{wf}$. $\mathtt{dom}(P_2) \cap \mathtt{dom}(P_3) = \emptyset$, so by (WF-Let) $\mathtt{let}\ x = P_2\ \mathtt{in}\ \ P_3 : \mathtt{wf}$ and $\mathtt{dom}(\mathtt{let}\ y = P_2\ \mathtt{in}\ \ P_3) \cap \mathtt{dom}(P_1) = \emptyset$ thus $\mathtt{let}\ y = P_1\ \mathtt{in}\ \ (\mathtt{let}\ x = P_2\ \mathtt{in}\ \ P_3) : \mathtt{wf}$. $\mathtt{dom}(\mathtt{let}\ x = (\mathtt{let}\ y = P_1\ \mathtt{in}\ \ P_2)\ \mathtt{in}\ \ P_3) = \mathtt{dom}(P_1) \cup \mathtt{dom}(P_2) \cup \mathtt{dom}(P_3) = \mathtt{dom}(\mathtt{let}\ y = P_1\ \mathtt{in}\ \ (\mathtt{let}\ x = P_2\ \mathtt{in}\ \ P_3))$.

$\square$

Proposition 3 (well formed substitution) $R : \mathtt{wf}$ *implies* $R\{x \leftarrow \ell\} : \mathtt{wf}$ *and* $\mathtt{dom}(R) = \mathtt{dom}(R\{x \leftarrow \ell\})$.

Proof. By induction on the depth of the derivation of $R : \mathtt{wf}$; we consider the last rule applied:

(WF-Exp) $e\{x \leftarrow \ell\} : \mathtt{wf}$ by (WF-Exp) and $\mathtt{dom}(e) = \mathtt{dom}(e\{x \leftarrow \ell\}) = \emptyset$;

(WF-Let) $\mathtt{let}\, y = P\, \mathtt{in}\, Q : \mathtt{wf}$ implies $P : \mathtt{wf}$, $Q : \mathtt{wf}$ and $\mathtt{dom}(P) \cap \mathtt{dom}(Q) = \emptyset$. By induction $P\{x \leftarrow \ell\} : \mathtt{wf}$, $\mathtt{dom}(P) = \mathtt{dom}(P\{x \leftarrow \ell\})$, $Q\{x \leftarrow \ell\} : \mathtt{wf}$ and $\mathtt{dom}(Q) = \mathtt{dom}(Q\{x \leftarrow \ell\})$. By (WF-Let) $\mathtt{let}\ y = P\{x \leftarrow \ell\}\ \mathtt{in}\ Q\{x \leftarrow \ell\} = (\mathtt{let}\ y = P\ \mathtt{in}\ Q)\{x \leftarrow \ell\} : \mathtt{wf}$ and $\mathtt{dom}(\mathtt{let}\, y = P\, \mathtt{in}\, Q) = \mathtt{dom}(P) \cup \mathtt{dom}(Q) = \mathtt{dom}(P\{x \leftarrow \ell\}) \cup \mathtt{dom}(Q\{x \leftarrow \ell\}) = (\mathtt{let}\, y = P\ \mathtt{in}\ Q)\{x \leftarrow \ell\}$;

(WF-Resource) $\langle\, \ell' \mapsto d \,\rangle$: $\texttt{wf}$; $(\langle\, \ell' \mapsto d \,\rangle)\{x{\leftarrow}\ell\} = \langle\, \ell' \mapsto d\{x{\leftarrow}\ell\} \,\rangle$: $\texttt{wf}$. $\texttt{dom}(\langle\, \ell' \mapsto d \,\rangle) = \texttt{dom}(\langle\, \ell' \mapsto d\{x{\leftarrow}\ell\} \,\rangle) = \{\ell'\}$;

(WF-Par) $P_1 \Rsh P_2$: $\texttt{wf}$ implies P_1 : $\texttt{wf}$, P_2 : $\texttt{wf}$ and $\texttt{dom}(P_1) \cap \texttt{dom}(P_2) = \emptyset$. By induction $P_1\{x{\leftarrow}\ell\}$: $\texttt{wf}$, $P_2\{x{\leftarrow}\ell\}$: $\texttt{wf}$, $\texttt{dom}(P_1) = \texttt{dom}(P_1\{x{\leftarrow}\ell\})$ and $\texttt{dom}(P_2) = \texttt{dom}(P_2\{x{\leftarrow}\ell\})$. By (WF-Par) $P_1\{x{\leftarrow}\ell\} \Rsh P_2\{x{\leftarrow}\ell\} = (P_1 \Rsh P_2)\{x{\leftarrow}\ell\}$: $\texttt{wf}$ and $\texttt{dom}(P_1 \Rsh P_2) = \texttt{dom}(P_1) \cup \texttt{dom}(P_2) = \texttt{dom}(P_1\{x{\leftarrow}\ell\}) \cup \texttt{dom}(P_2\{x{\leftarrow}\ell\}) = \texttt{dom}((P_1 \Rsh P_2)\{x{\leftarrow}\ell\})$;

(WF-Res) $(\nu\ell)'P$: $\texttt{wf}$ implies P : $\texttt{wf}$ and $\ell' \in \texttt{dom}(P)$. By induction $P\{x{\leftarrow}\ell\}$: $\texttt{wf}$ and $\texttt{dom}(P) = \texttt{dom}(P\{x{\leftarrow}\ell\})$, thus by (WF-Res) $(\nu\ell)'P\{x{\leftarrow}\ell\}$: $\texttt{wf}$ and $\texttt{dom}((\nu\ell)'P) = \texttt{dom}(P) \setminus \{\ell'\} = \texttt{dom}(P\{x{\leftarrow}\ell\}) \setminus \{\ell'\} = \texttt{dom}(((\nu\ell)'P)\{x{\leftarrow}\ell\})$.

$\square$

Theorem 4 (well formed subject reduction) *Suppose* P : $\texttt{wf}$, *if* $P \to Q$ *then* Q : $\texttt{wf}$ *and* $\texttt{dom}(P) = \texttt{dom}(Q)$.

Proof. By induction on the depth of the derivation of $P \to Q$; we distinguish the last rule applied:

(Red Fun) $f(\vec{u})$: $\texttt{wf}$ (WF-Exp) and $\texttt{dom}(f(\vec{u})) = \emptyset$. $f(\vec{u}) \to e\{\vec{x}{\leftarrow}\vec{u}\}$, $e\{\vec{x}{\leftarrow}\vec{u}\}$: $\texttt{wf}$ by (WF-Exp) and $\texttt{dom}(e\{\vec{x}{\leftarrow}\vec{u}\}) = \emptyset$;

(Red Let) $\texttt{let}\ x = u\ \texttt{in}\ P$: $\texttt{wf}$ implies u : $\texttt{wf}$ and P : $\texttt{wf}$; moreover $\texttt{dom}(u) = \emptyset$ because u is an expression. $\texttt{let}\ x = u\ \texttt{in}\ P \to P\{x{\leftarrow}u\}$; by Proposition 3 $P\{x{\leftarrow}u\}$: $\texttt{wf}$ and $\texttt{dom}(P) = \texttt{dom}(P\{x{\leftarrow}u\})$;

(Red Struct) P : $\texttt{wf}$ and $P \equiv Q$ imply Q : $\texttt{wf}$ and $\texttt{dom}(P) = \texttt{dom}(Q)$ by Proposition 2. By induction, $Q \to Q'$ implies Q' : $\texttt{wf}$ and $\texttt{dom}(Q) = \texttt{dom}(Q')$; finally, by Proposition 2, $Q' \equiv P'$ implies P' : $\texttt{wf}$ and $\texttt{dom}(P') = \texttt{dom}(Q') = \texttt{dom}(Q) = \texttt{dom}(P)$;

(Red Context) by a straightforward induction on the derivation of P : $\texttt{wf}$, distinguishing the context E;

(Red Ref) $\texttt{newref}\ u$: $\texttt{wf}$ and $\texttt{dom}(\texttt{newref}\ u) = \emptyset$, because it is an expression. $\texttt{newref}\ u \to (\nu\ell)(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell)$; by (WF-Exp) ℓ : $\texttt{wf}$ and $\texttt{dom}(\ell) = \emptyset$, by (WF-Resource) $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle$: $\texttt{wf}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle) = \{\ell\}$, by (WF-Par) $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell$: $\texttt{wf}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell) = \{\ell\}$ and finally, by (WF-Res) $(\nu\ell)(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell)$: $\texttt{wf}$ and $\texttt{dom}((\nu\ell)(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh \ell)) = \emptyset = \texttt{dom}(\texttt{newref}\ u)$;

(Red Read) $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh !\ell$: $\texttt{wf}$ implies, by rule (WF-Par), $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle$: $\texttt{wf}$ and $!\ell$: $\texttt{wf}$; moreover $\texttt{dom}(!\ell) = \emptyset$ because it is an expression. $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh !\ell \to \langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh u$, u : $\texttt{wf}$ by rule (WF-Exp), and $\texttt{dom}(u) = \emptyset$. In conclusion, $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh u$: $\texttt{wf}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh u) = \texttt{dom}(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \Rsh !\ell) = \{\ell\}$;

(Red Write) $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \upharpoonright \ell \mathrel{+}= v : \texttt{wf}$ implies, by rule (WF-Par), $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle : \texttt{wf}$ and $\ell \mathrel{+}= v : \texttt{wf}$; moreover $\texttt{dom}(\ell \mathrel{+}= v) = \emptyset$ because it is an expression. $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \upharpoonright \ell \mathrel{+}= v \to \langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \upharpoonright \texttt{()};\ \texttt{()} : \texttt{wf}$ by rule (WF-Exp), and $\texttt{dom}(\texttt{()}) = \emptyset$. In conclusion, $\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \upharpoonright \texttt{()} : \texttt{wf}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \upharpoonright \texttt{()}) = \texttt{dom}(\langle\, \ell \mapsto \texttt{ref}\ u \,\rangle \upharpoonright \ell \mathrel{+}= v) = \{\ell\}$;

(Red Node) $\texttt{a}[u] : \texttt{wf}$ and $\texttt{dom}(\texttt{a}[u]) = \emptyset$ because it is an expression. $\texttt{a}[u] \to (\nu\imath)(\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle \upharpoonright \imath)$; by rule (WF-Exp) $\imath : \texttt{wf}$ and $\texttt{dom}(\imath) = \emptyset$ because it is an expression, by (WF-Resource) $\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle : \texttt{wf}$ and $\texttt{dom}(\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle) = \{\imath\}$, by (WF-Par) $\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle \upharpoonright \imath : \texttt{wf}$ and $\texttt{dom}(\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle \upharpoonright \imath) = \{\imath\}$, finally, by (WF-Res), $(\nu\imath)(\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle \upharpoonright \imath) : \texttt{wf}$ and $\texttt{dom}((\nu\imath)(\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle \upharpoonright \imath)) = \texttt{dom}(\langle\, \imath \mapsto \texttt{node}\ \texttt{a}(u) \,\rangle \upharpoonright \imath) \setminus \{\imath\} = \emptyset = \texttt{dom}(\texttt{a}[u])$;

(Red Comp) $u_1, u_2 : \texttt{wf}$ and $\texttt{dom}(u_1, u_2) = \emptyset$. $u_1, u_2 \to \imath_1 \ldots \imath_n$; by (WF-Exp) $\imath_1 \ldots \imath_n : \texttt{wf}$ and $\texttt{dom}(\imath_1 \ldots \imath_n) = \texttt{dom}(u_1, u_2) = \emptyset$;

(Red Try) $\texttt{try}\ u\ p(\vec{v}) : \texttt{wf}$ and $\texttt{dom}(\texttt{try}\ u\ p(\vec{v})) = \emptyset$ because it is an expression. $\texttt{try}\ u\ p(\vec{v}) \to (\nu\imath, \ell)(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \upharpoonright \ell)$; by (WF-Exp) $\ell : \texttt{wf}$ and $\texttt{dom}(\ell) = \emptyset$ because it is an expression, by (WF-Resource) $\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle : \texttt{wf}$, $\langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{u}) \,\rangle : \texttt{wf}$, $\texttt{dom}(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle) = \{\imath\}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{u}) \,\rangle) = \ell$. By (WF-Par) $\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \upharpoonright \ell : \texttt{wf}$ and $\texttt{dom}(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \upharpoonright \ell) = \{\imath, \ell\}$ and by (WF-Res) $(\nu\imath, \ell)(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \upharpoonright \ell) : wf$ and $\texttt{dom}((\nu\imath, \ell)(\langle\, \imath \mapsto \texttt{node}\ \boldsymbol{o}(u) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \upharpoonright \ell)) = \emptyset$;

(Red Try Match) $P \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle : \texttt{wf}$ implies, by (WF-Par), $P : \texttt{wf}$, $\langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle : \texttt{wf}$, and $\texttt{dom}(P) \cap \texttt{dom}(\langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle) = \emptyset$. $P \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \to P \upharpoonright (\nu\jmath_1 \ldots \jmath_n)\big(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle\big)$; by (WF-Resource) $\langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle : \texttt{wf}$ and $\forall k \in 1 \ldots n\ \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle : \texttt{wf}$. $\texttt{dom}(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle) = \{\jmath_1, \ldots, \jmath_n\}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle) = \ell$, thus $\texttt{dom}(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle) \cap \texttt{dom}(\langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle) = \emptyset$ and by (WF-Par) $\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle : \texttt{wf}$. By (WF-Res) $(\nu\jmath_1, \ldots, \jmath_n)\big(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle\big) : \texttt{wf}$ and by (WF-Par) $P \upharpoonright (\nu\jmath_1 \ldots \jmath_n)\big(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle\big) : \texttt{wf}$ because $\texttt{dom}(P) \cap \texttt{dom}((\nu\jmath_1 \ldots \jmath_n)\big(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle\big)) = \emptyset$. Moreover $\texttt{dom}(P \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle) = \texttt{dom}(P) \cup \{\ell\} = \texttt{dom}(P \upharpoonright (\nu\jmath_1 \ldots \jmath_n)\big(\prod_{k\in 1..n} \langle\, \jmath_k \mapsto \texttt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \upharpoonright \langle\, \ell \mapsto \texttt{test}\ \imath\ \jmath_1 \ldots \jmath_n \,\rangle\big))$

(Red Try All) $\langle\, \ell \mapsto \texttt{try}\ \imath\ \texttt{All} \,\rangle : \texttt{wf}$ and $\texttt{dom}(\langle\, \ell \mapsto \texttt{try}\ \imath\ \texttt{All} \,\rangle) = \{\ell\}$. $\langle\, \ell \mapsto \texttt{try}\ \imath\ \texttt{All} \,\rangle \to \langle\, \ell \mapsto \texttt{ok}\ \imath \rangle$; $\langle\, \ell \mapsto \texttt{ok}\ \imath \rangle : \texttt{wf}$ by (WF-Resource) and $\texttt{dom}(\langle\, \ell \mapsto \texttt{ok}\ \imath \rangle) = \{\ell\} = \texttt{dom}(\langle\, \ell \mapsto \texttt{try}\ \imath\ \texttt{All} \,\rangle)$;

(Red Try Error) $P \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle : \texttt{wf}$ implies, by (WF-Par), $P : \texttt{wf}$, $\langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle : \texttt{wf}$ and $\texttt{dom}(P) \cap \texttt{dom}(\langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle) = \emptyset$. $P \upharpoonright \langle\, \ell \mapsto \texttt{try}\ \imath\ p(\vec{v}) \,\rangle \to P \upharpoonright \langle\, \ell \mapsto \texttt{fail}\ \imath \rangle$; by (WF-Resource) $\langle\, \ell \mapsto \texttt{fail}\ \imath \rangle : \texttt{wf}$, moreover $\texttt{dom}(\langle\, \ell \mapsto \texttt{fail}\ \imath \rangle) =$

$\mathtt{dom}(\langle\, \ell \mapsto \mathtt{try}\, \imath\, p(\vec{v})\,\rangle) = \{\ell\}$, thus $\mathtt{dom}(P) \cap \mathtt{dom}(\langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle) = \emptyset$ and by (WF-Par) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle : \mathtt{wf}$;

(Red Test Ok) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle : \mathtt{wf}$ implies, by (WF-Par), $P : \mathtt{wf}$, $\langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle : \mathtt{wf}$ and $\mathtt{dom}(P) \cap \mathtt{dom}(\langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle) = \emptyset$. $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle \rightarrow P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{ok}\, \imath\,\rangle$; by (WF-Resource) $\langle\, \ell \mapsto \mathtt{ok}\, \imath\,\rangle : \mathtt{wf}$, moreover $\mathtt{dom}(\langle\, \ell \mapsto \mathtt{ok}\, \imath\,\rangle) = \mathtt{dom}(\langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle) = \{\ell\}$, thus $\mathtt{dom}(P) \cap \mathtt{dom}(\langle\, \ell \mapsto \mathtt{ok}\, \imath\,\rangle) = \emptyset$ and by (WF-Par) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{ok}\, \imath\,\rangle : \mathtt{wf}$;

(Red Test Fail) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle : \mathtt{wf}$ implies, by (WF-Par), $P : \mathtt{wf}$, $\langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle : \mathtt{wf}$ and $\mathtt{dom}(P) \cap \mathtt{dom}(\langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle) = \emptyset$. $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle \rightarrow P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle$; by (WF-Resource) $\langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle : \mathtt{wf}$, moreover $\mathtt{dom}(\langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle) = \mathtt{dom}(\langle\, \ell \mapsto \mathtt{test}\, \imath\, w\,\rangle) = \{\ell\}$, thus $\mathtt{dom}(P) \cap \mathtt{dom}(\langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle) = \emptyset$ and by (WF-Par) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \langle\, \ell \mapsto \mathtt{fail}\, \imath\,\rangle : \mathtt{wf}$;

(Red Wait Ok) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 : \mathtt{wf}$ implies, by (WF-Par), $P : \mathtt{wf}$, $\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$ and $\mathtt{dom}(P) \cap \mathtt{dom}(\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2) = \emptyset$. $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \rightarrow P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, e_1\{x \leftarrow u\}$; $e_1\{x \leftarrow u\} : \mathtt{wf}$ because $e_1 : \mathtt{wf}$ (WF-Exp) and by Proposition 3, moreover $\mathtt{dom}(e_1\{x \leftarrow u\}) = \emptyset$, thus, by rule (WF-Par), $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, e_1\{x \leftarrow u\} : \mathtt{wf}$;

(Red Wait Fail) $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 : \mathtt{wf}$ implies, by (WF-Par), $P : \mathtt{wf}$, $\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$ and $\mathtt{dom}(P) \cap \mathtt{dom}(\mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2) = \emptyset$. $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, \mathtt{wait}\ \ell(x)\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \rightarrow P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, e_2\{x \leftarrow u\}$; $e_2\{x \leftarrow u\} : \mathtt{wf}$ because $e_2 : \mathtt{wf}$ (WF-Exp) and by Proposition 3, moreover $\mathtt{dom}(e_2\{x \leftarrow u\}) = \emptyset$, thus, by rule (WF-Par), $P \,\mathbin{\lceil\!\!\!\!\!\rightarrow}\, e_2\{x \leftarrow u\} : \mathtt{wf}$.

$\square$

B Proof of Theorem 1

We are set to prove the main result of the paper, the subject reduction theorem; but we need a few preliminary results.

Proposition 5 (substitution) *If $E, x{:}t \vdash P : t'$ and $E \vdash u : t$ then $E \vdash P\{x \leftarrow u\} : t'$.*

Proof. By a straightforward induction on the derivation of $E, x{:}t \vdash P : t'$. $\square$

Proposition 6 (weakening) *If $E, x{:}t \vdash P : t'$ and $x \notin fn(P)$ then $E \vdash P : t'$ and vice versa.*

Proof. By a straightforward induction on the derivation of $E, x{:}t \vdash P : t'$. $\square$

Proposition 7 (subject congruence) *If $P \equiv Q$ and $E \vdash P : t$ then $E \vdash Q : t$.*

Proof. By induction on the depth of the derivation of $P \equiv Q$; we consider the last structural congruence rule applied:

(Struct Par Assoc) $E \vdash (P_1 \Rsh P_2) \Rsh P_3 : t_3$ implies, by rule (Type Par), $E \vdash P_3 : t_3$ and $E \vdash P_1 \Rsh P_2 : t_2$. Again, $E \vdash P_1 : t_1$ and $E \vdash P_2 : t_2$. By the same rule $E \vdash P_2 \Rsh P_3 : t_3$ and $E \vdash P_1 \Rsh (P_2 \Rsh P_3) : t_3$;

(Struct Par Let) $E \vdash P_1 \Rsh \texttt{let}\ x = P_2\ \texttt{in}\ P_3 : t_3$ implies, by (Type Par) and (Type Let), $E \vdash P_1 : t_1$, $E \vdash P_2 : t_2$ and $E, x{:}t_2 \vdash P_3 : t_3$. By (Type Par) $E \vdash P_1 \Rsh P_2 : t_2$ and by (Type Let) $E \vdash \texttt{let}\ x = P_1 \Rsh P_2\ \texttt{in}\ P_3 : t_3$;

(Struct Par Comm) this case is similar to (Struct Par Assoc);

(Struct Res Let) $E \vdash (\nu\ell)\texttt{let}\ x = P_1\ \texttt{in}\ P_2 : t_2$ implies, by (Type Res), $E, \ell{:}t' \vdash \texttt{let}\ x = P_1\ \texttt{in}\ P_2 : t_2$. By (Type Let) we have $E, \ell{:}t' \vdash P_1 : t_1$ and $E, \ell{:}t', x{:}t_1 \vdash P_2 : t_2$. By (Type Res) $E \vdash (\nu\ell)P_1 : t_1$ and by Proposition 6 (weakening) $E, x{:}t_1 \vdash P_2 : t_2$ and by rule (Type Let) $E \vdash \texttt{let}\ x = (\nu\ell)P_1\ \texttt{in}\ P_2 : t$;

(Struct Res Res) $E \vdash (\nu\ell)(\nu\imath)R : t'$ implies, by rule (Type Res), $E, \ell{:}t_1 \vdash (\nu\imath)R : t'$, and again $E, \ell{:}t_1, \imath{:}t_2 \vdash R : t'$. By the same rule $E, \imath{:}t_2 \vdash (\nu\ell)R : t'$ and $E \vdash (\nu\imath)(\nu\ell)R : t'$;

(Struct Res Par R) $E \vdash (\nu\imath)(P_1 \Rsh P_2) : t_2$ implies, by rule (Type Res), $E, \imath{:}t' \vdash P_1 \Rsh P_2 : t_2$ and, by (Type Par), $E, \imath{:}t' \vdash P_1 : t_1$ and $E, \imath{:}t' \vdash P_2 : t_2$. By (Type Res) $E \vdash (\nu\imath)P_2 : t_2$, by Proposition 6 (weakening) $E \vdash P_1 : t_1$ and by rule (Type Par) $E \vdash P_1 \Rsh (\nu\imath)P_2 : t_2$;

(Struct Res Par L) this case is similar to the previous;

(Struct Let Assoc) $E \vdash \texttt{let}\ x = (\texttt{let}\ y = P_1\ \texttt{in}\ P_2)\ \texttt{in}\ P_3 : t$ implies, by rule (Type Let), $E \vdash \texttt{let}\ y = P_1\ \texttt{in}\ P_2 : t_2$ and $E, x{:}t_2 \vdash P_3 : t_3$. Again, $E \vdash P_1 : t_1$ and $E, y{:}t_1 \vdash P_2 : t_2$. By (Struct Let Assoc) $y \notin \mathit{fn}(P_3)$ so, by Proposition 6 (weakening), we have $E, y{:}t_1, x{:}t_2 \vdash P_3 : t_3$, so by (Type Let) $E \vdash \texttt{let}\ y = P_1\ \texttt{in}\ (\texttt{let}\ x = P_2\ \texttt{in}\ P_3) : t$.

$\square$

Proposition 8 *Assume* $S = \mathit{Reg}(\mathtt{a_i}[p_i(\vec{v_i})])_{i\in 1..k}$ *is a unambiguous pattern with type* A. *If* $\mathtt{a_1}\dots\mathtt{a_n} \vdash_S p_1(\vec{v_1})\dots p_n(\vec{v_n})$ *then we also have* $\mathtt{a_1}\dots\mathtt{a_n} \vdash_A A_1\dots A_n$.

Proof. $E \vdash \mathit{Reg}(\mathtt{a_i}[p_i(\vec{v_i})])_{i=1,\dots,k} : A$ implies $\forall i :\ p_i : (\vec{t_i}) \to A_i$, $E \vdash \vec{v_i} : \vec{t_i}$, and $\mathit{Reg}(\mathtt{a_i}[A_i])_{i=1,\dots,k} \doteq A$. $\mathtt{a_1}\dots\mathtt{a_n} \vdash_S p_1(\vec{v_1})\dots p_n(\vec{v_n})$ implies that $\mathtt{a_1}\dots\mathtt{a_n} \in \mathit{Reg}(\mathtt{a_i})_{i=1,\dots,k}$. Moreover, S is unambiguous, thus for every tag $\mathtt{a_i}$ we have exactly one pattern $p_i(\vec{v_i})$, s.t. $p_i : (\vec{t_i}) \to A_i$ and $E \vdash \vec{v_i} : \vec{t_i}$ thus in A for every tag $\mathtt{a_i}$ we have associated exactly the type A_i, and $\mathtt{a_1}\dots\mathtt{a_n} \vdash_A A_1\dots A_n$. $\square$

Proposition 9 *Assume* A *is a an unambiguous type. If* $\mathtt{a_1}\dots\mathtt{a_n} \vdash_A A_1\dots A_n$ *then* $\mathtt{a_1}[A_1], \dots, \mathtt{a_n}[A_n] <: A$ *and if* $\mathtt{a_1}\dots\mathtt{a_n} \not\vdash_A$ *then there is no* $B_1,\dots,B_n$ *such that* $\mathtt{a_1}[B_1], \dots, \mathtt{a_n}[B_n] <: A$.

Proof. By definition of (type) witness. □

Proposition 10 *Suppose A unambiguous and $A \neq$ `All`. $\mathtt{a_1} \ldots \mathtt{a_j} \ldots \mathtt{a_n} \vdash_A A_1 \ldots A_j \ldots A_n \Rightarrow \mathtt{a_1}[A_1], \ldots, \mathtt{a_j}[\overline{A_j}], \ldots, \mathtt{a_n}[A_n] <: \overline{A}$.*

Proof. By Proposition 9, $a_1 \ldots a_j \ldots a_n \vdash_A A_1 \ldots A_j \ldots A_n$ implies $a_1[A_1], \ldots, a_j[A_j], \ldots, a_n[A_n] <: A$, that is $\mathcal{L}(a_1[A_1], \ldots, a_j[A_j], \ldots, a_n[A_n]) \subseteq \mathcal{L}(A)$.

$\forall d \in (a_1[A_1], \ldots, a_j[\overline{A_j}], \ldots, a_n[A_n]) : d \notin (a_1[A_1], \ldots, a_j[A_j], \ldots, a_n[A_n])$ because $\mathcal{L}(\overline{A_j}) = \overline{\mathcal{L}(A_j)}$, that is $\mathcal{L}(\overline{A_j}) \cap \mathcal{L}(A_j) = \emptyset$. Thus, by the unambiguity, $\forall d \in a_1[A_1], \ldots, a_j[\overline{A_j}], \ldots, a_n[A_n]$ we have $d \notin A$ that is $\mathcal{L}(a_1[A_1], \ldots, a_j[\overline{A_j}], \ldots, a_n[A_n]) \cap \mathcal{L}(A) = \emptyset$. In conclusion, $\mathcal{L}(a_1[A_1], \ldots, a_j[\overline{A_j}], \ldots, a_n[A_n]) \subseteq \mathcal{L}(\overline{A})$ and $a_1[A_1], \ldots, a_j[\overline{A_j}], \ldots, a_n[A_n] <: \overline{A}$. □

Proposition 11 *If $a_1[d_1] \ldots a_n[d_n] \in A$ then $A = a_1[d_1], \ldots, a_n[d_n] \,|\, A$.*

Definition 2 ($[\![u]\!]_E$)
$[\![()]\!]_E = ()$
$[\![\imath_1 \ldots \imath_n]\!]_E = a_1[d_1] \ldots a_n[d_n]$ *if* $E \vdash \imath_i : \mathtt{node}\ \mathtt{a_i}(u_i)$ *and* $[\![u_i]\!]_E = d_i$.

Proposition 12 *$E \vdash u : A$ and $u = \imath_1 \ldots \imath_n \Leftrightarrow [\![u]\!]_E \in A$.*

Proof.

($\Rightarrow$): By induction on the depth of u:

- $d = 0$**:** In this case $u = (\,)$ and $[\![(\,)]\!]_E = (\,)$. $E \vdash (\,) :$ `Empty` and $(\,) \in$ `Empty`.
- $d = n + 1$**:** In this case $u = \imath_1 \ldots \imath_n$. If the last rule applied for deducing that $E \vdash u : A$ is (Type Doc), we have:
  - $A = a_1[B_1], \ldots, a_n[B_n]$;
  - $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(u_k)$;
  - $E \vdash u_k : B_k$; every u_k has depth less or equal to n, thus by induction $[\![u_k]\!]_E \in B_k$.

  If the last rule applied for deducing that $E \vdash u : A$ is (Type Sub), we have:
  - $E \vdash u : a_1[B_1], \ldots, a_n[B_n]$, that is $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(u_k)$, and $E \vdash u_k : B_k$; every u_k has depth less or equal to n, thus by induction $[\![u_k]\!]_E \in B_k$.
  - $a_1[B_1], \ldots, a_n[B_n] <: A$ implies $\mathcal{L}(a_1[B_1], \ldots, a_n[B_n]) \subseteq \mathcal{L}(A)$.

  In both cases, $[\![u]\!]_E = a_1[[\![u_1]\!]_E] \ldots a_n[[\![u_n]\!]_E] \in a_1[B_1], \ldots, a_n[B_n]$, thus $[\![u]\!]_E \in A$.

($\Leftarrow$): By induction on the depth of u:

- $d = 0$**:** In this case $u = (\,)$ and $[\![(\,)]\!]_E = (\,)$. $(\,) \in A$ implies $\mathcal{L}(\mathtt{Empty}) \subseteq \mathcal{L}(A)$. $E \vdash (\,) :$ `Empty` and by (Type Sub) `Empty` $<: A$ implies $E \vdash (\,) : A$.

$d = n+1$**:** In this case $u = \imath_1 \dots \imath_n$. $[\![u]\!]_E = a_1[d_1] \dots a_n[d_n] \in A$ with $d_1 = [\![u_1]\!]_E$, $\dots$, $d_n = [\![u_n]\!]_E$. We can say that $\forall i : \ d_i \in d_i$ and by induction $E \vdash d_i : d_i$. $a_1[d_1] \dots a_n[d_n] \in A$ implies, by Proposition 11, $A = a_1[d_1], \dots, a_n[d_n] \mid A$. In conclusion $a_1[d_1], \dots, a_n[d_n] <: A$ and by rules (Type Doc) and (Type Sub) $E \vdash u : A$.

$\square$

Proposition 13 *Suppose $E \vdash S : A$ and $u = \imath_1 \dots \imath_n$ with $E \vdash \imath_i : \texttt{node}\ \mathtt{a_i}(u_i)$ for $i \in 1, \dots, n$. If $\mathtt{a_1} \dots \mathtt{a_n} \not\vdash_S$ then $E \vdash u : \overline{A}$.*

Proof. Suppose $S = \mathit{Reg}(\mathtt{a'_i}[p_i(\vec{v_i})])_{i \in 1,\dots,k}$. $E \vdash S : A$ implies $p_i : (\vec{t_i}) \to A_i$, $E \vdash \vec{v_i} : \vec{t_i}$ and $A \doteq \mathit{Reg}(\mathtt{a'_i}[A_i])_{i \in 1,\dots,k}$.
$\mathtt{a_1} \dots \mathtt{a_n} \not\vdash_S$ means that $\mathtt{a_1} \dots \mathtt{a_n} \notin \mathit{Reg}(\mathtt{a'_i})_{i \in 1,\dots,k}$, so by definition $\mathtt{a_1} \dots \mathtt{a_n} \not\vdash_A$ and by Proposition 9 $\forall B_i : \ \mathtt{a_1}[B_1], \dots, \mathtt{a_n}[B_n] \not<: A$. We can not apply rule (Term Sub) for saying that $E \vdash u : A$, so $E \not\vdash u : A$. By Proposition 12, this means that $[\![u]\!]_E \notin A$ that is $[\![u]\!]_E \in \overline{A}$, and by Proposition 12 $E \vdash u : \overline{A}$. $\square$

Theorem 14 (Theorem 1) *Suppose that P is well formed and contains only unambiguous patterns and t contains only unambiguous types. If $E \vdash P : t$ and $P \to Q$ then $E \vdash Q : t$.*

Proof. By induction on reduction rules. We distinguish the last rule applied (rememebr that at every step we work with a well formed term):

(Red Fun) by rule (Type Fun) $E \vdash f(u_1, \dots, u_n) : t_0$ implies $f : (t_1, \dots, t_n) \to t_0$ and $E \vdash u_i : t_i$. $f : (t_1, \dots, t_n) \to t_0$ means that $f(x_1, \dots, x_n) := e$ and $x_1{:}t_1, \dots, x_n{:}t_n \vdash e : t_0$. By (Red Fun) $f(u_1, \dots, u_n) \to e\{x_1 \leftarrow u_1\} \dots \{x_n \leftarrow u_n\}$; in conclusion, by Proposition 5 (substitution), $x_1{:}t_1, \dots, x_n{:}t_n \vdash e : t_0$ and $E \vdash u_i : t_i$ implies $E \vdash e\{x_1 \leftarrow u_1\} \dots \{x_n \leftarrow u_n\} : t_0$;

(Red Let) by rule (Type Let) $E \vdash \texttt{let}\ x = u\ \texttt{in}\ P : t'$ implies $E \vdash u : t$ and $E, x : t \vdash P : t'$; by Proposition 5 (substitution) $E \vdash P\{x \leftarrow u\} : t'$;

(Red Struct) if $P : t$ and $P \equiv Q$ by Proposition 7 (subject congruence) $Q : t$. By induction $Q \to Q'$ and $Q' : t$. Again for Proposition 7 (subject congruence), $Q' \equiv P'$ implies $P' : t$;

(Red Context) the proof is straightforward distinguishing the context E;

(Red Ref) by rule (Type Ref) $E \vdash \texttt{newref}\ u : \texttt{ref}\ A$ implies $E \vdash u : A$. By (Red Ref) $\texttt{newref}\ u \to (\nu\ell)(\langle \ell \mapsto \texttt{ref}\ u \rangle \Rsh \ell)$. If we consider $\ell : \texttt{ref}\ A$, and using rules (Type Res), (Type Par), (Type Loc Ref) and (Type x) $E \vdash (\nu\ell)(\langle \ell \mapsto \texttt{ref}\ u \rangle \Rsh \ell) : \texttt{ref}\ A$;

(Red Read) by rules (Type Loc Ref) and (Type Read) $E \vdash \langle \ell \mapsto \texttt{ref}\ u \rangle \Rsh !\ell : A$ implies $E \vdash \ell : \texttt{ref}\ A$, and $E \vdash u : A$. Using rules (Type Loc Ref), (Type x) and (Type Par) $E \vdash \langle \ell \mapsto \texttt{ref}\ u \rangle \Rsh u : A$;

(Red Write) by rules (Type Loc Ref) and (Type Write) $E \vdash \langle\, \ell \mapsto \mathtt{ref}\ u \,\rangle \Lsh l \mathrel{+}= v : \mathtt{Empty}$ implies $E \vdash \ell : \mathtt{ref}\ A$, $E \vdash u : A$, $E \vdash v : B$ and $A, B <: A$. Rule (Red Write) implies $u, v = w$ and by (Type Comp) $E \vdash w : A, B$, thus $A, B <: A$ implies $E \vdash w : A$ and $E \vdash \langle\, \ell \mapsto \mathtt{ref}\ w \,\rangle : \star$, by rules (Type Loc Ref) and $E \vdash \langle\, \ell \mapsto \mathtt{ref}\ w \,\rangle \Lsh \mathtt{()} : \mathtt{Empty}$ by rule (Type Par);

(Red Node) $E \vdash \mathtt{a}[u] : \mathtt{a}[A]$ implies, by (Type Node), $E \vdash u : A$. If we consider $\imath : \mathtt{node}\ \mathtt{a}(u)$, by (Red Node) $\mathtt{a}[u] \rightarrow (\nu\imath)(\langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(u) \,\rangle \Lsh \imath)$ implies $u = \imath_1 \ldots \imath_n$, and by rules (Type Res), (Type Par), (Type Loc Node), and (Type Doc) $E \vdash (\nu\imath)(\langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(u) \,\rangle \Lsh \imath) : \mathtt{a}[A]$;

(Red Comp) by rule (Type Comp) $E \vdash u_1, u_2 : A_1, A_2$ implies $E \vdash u_i : A_i$ for $i = 1, 2$. By (Red Comp) $u_1 = \imath_1 \ldots \imath_k$ and $u_2 = \imath_{k+1} \ldots \imath_n$.

If we have deduced $E \vdash u_1 : A_1$ and $E \vdash u_2 : A_2$ both by using rule (Type Doc), then $A_1 = a_1[B_1], \ldots, a_k[B_k]$ and $A_2 = a_{k+1}[B_{k+1}], \ldots, a_n[B_n]$, and by (Type Doc) $E \vdash \imath_1 \ldots \imath_k \imath_{k+1} \ldots \imath_n : A_1, A_2$.

If we have deduced $E \vdash u_1 : A_1$ and $E \vdash u_2 : A_2$ both by using rule (Type Sub), then $a_1[B_1], \ldots, a_k[B_k] <: A_1$ and $a_{k+1}[B_{k+1}], \ldots, a_n[B_n] <: A_2$, and by (Type Doc) $E \vdash u_1 : a_1[B_1], \ldots, a_k[B_k]$ and $E \vdash u_2 : a_{k+1}[B_{k+1}], \ldots, a_n[B_n]$. By (Type Doc) $E \vdash \imath_1 \ldots \imath_k \imath_{k+1} \ldots \imath_n : a_1[B_1], \ldots, a_k[B_k], a_{k+1}[B_{k+1}], \ldots, a_n[B_n]$. Moreover, $a_1[B_1], \ldots, a_k[B_k], a_{k+1}[B_{k+1}], \ldots, a_n[B_n] <: A_1, A_2$, and by (Type Sub) $E \vdash \imath_1 \ldots \imath_k \imath_{k+1} \ldots \imath_n : A_1, A_2$.

The cases $E \vdash u_1 : A_1$ by (Type Doc) and $E \vdash u_2 : A_2$ by (Type Sub) and vice versa, are similar to the previous;

(Red Try) by rule (Type Try Doc) $E \vdash \mathtt{try}\ u\ p(\vec{v}) : \mathtt{loc}\ \boldsymbol{o}(A)$ implies $p : (\vec{t}) \rightarrow A$, $E \vdash \vec{v} : \vec{t}$, and $E \vdash u : B$; by the reduction $u = \imath_1 \ldots \imath_n$. If we choose $\imath : \mathtt{node}\ \boldsymbol{o}(u)$ and $\ell : \mathtt{loc}\ \boldsymbol{o}(A)$ we have $E, \imath{:}\mathtt{node}\ \boldsymbol{o}(u) \vdash \langle\, \imath \mapsto \mathtt{node}\ \boldsymbol{o}(u) \,\rangle : \star$, by (Type Loc Node), and $E, \imath{:}\mathtt{node}\ \boldsymbol{o}(u), \ell{:}\mathtt{loc}\ \boldsymbol{o}(A) \vdash \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v}) \,\rangle : \star$. Finally, by rules (Type Res), (Type Par), and (Type x) $E \vdash (\nu\imath, \ell)(\langle\, \imath \mapsto \mathtt{node}\ \boldsymbol{o}(u) \,\rangle \Lsh \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v}) \,\rangle \Lsh \ell) : \mathtt{loc}\ \boldsymbol{o}(A)$;

(Red Try Match) by rules (Type Par), (Type Try Doc), and (Type Loc Node) $E \vdash \prod_{k \in 1 \ldots n} \langle\, \imath_k \mapsto \mathtt{node}\ \mathtt{a_k}(w_k) \,\rangle \Lsh \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n) \,\rangle \Lsh \langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v}) \,\rangle : \star$ implies:

- $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n)$;
- $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(w_k)$ and $w_k = (\imath_{1_k} \ldots \imath_{n_k})$;
- $E \vdash \ell : \mathtt{loc}\ \mathtt{a}(A)$, $p : (\vec{t}) \rightarrow A$, and $E \vdash \vec{v} : \vec{t}$; thus if $p(\vec{v}) := S$ then $S : A$.

By (Red Try Match) $\prod_{k \in 1 \ldots n} \langle\, \imath_k \mapsto \mathtt{node}\ \mathtt{a_k}(w_k) \,\rangle \Lsh \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n) \,\rangle \Lsh$ $\langle\, \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v}) \,\rangle \rightarrow \prod_{k \in 1 \ldots n} \langle\, \imath_k \mapsto \mathtt{node}\ \mathtt{a_k}(w_k) \,\rangle \Lsh \langle\, \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \ldots \imath_n) \,\rangle \Lsh$ $(\nu w)(\prod \langle\, \jmath_k \mapsto \mathtt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle \Lsh \langle\, \ell \mapsto \mathtt{test}\ \imath\ w \,\rangle)$ implies $w = \jmath_1 \ldots \jmath_n$ fresh and $\mathtt{a_1} \ldots \mathtt{a_n} \vdash_S p_1(\vec{v_1}) \ldots p_n(\vec{v_n})$.
If $p_k : (\vec{t_k}) \rightarrow A_k$ we choose $\jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)$ and $E, \jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)_{k=1,\ldots,n} \vdash \prod_k \langle\, \jmath_k \mapsto \mathtt{try}\ \imath_k\ p_k(\vec{v_k}) \,\rangle : \star$.
We have to show that $\langle\, \ell \mapsto \mathtt{test}\ \imath\ w \,\rangle : \star$. We know that:

- $E \vdash \ell : \mathtt{loc}\ \mathtt{a}(A)$;
- $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n)$;
- $\jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)_{k=1,\dots,n}$.

We have to prove that $\mathtt{a_1} \dots \mathtt{a_n} \vdash_A A_1 \dots A_n$. By the reduction we have $\mathtt{a_1} \dots \mathtt{a_n} \vdash_S p_1(\vec{v_1}) \dots p_n(\vec{v_n})$; moreover $p_i(\vec{v_i}) : A_i$, and $S : A$, so by Proposition 8 $\mathtt{a_1} \dots \mathtt{a_n} \vdash_A A_1 \dots A_n$, thus $E \vdash \langle \ell \mapsto \mathtt{test}\ \imath\ w \rangle : \star$. In conclusion $E \vdash (\nu w)(\prod \langle \jmath_k \mapsto \mathtt{try}\ \imath_k\ p_k(\vec{v_k}) \rangle \upharpoonright \langle \ell \mapsto \mathtt{test}\ \imath\ w \rangle) : \star$;

(Red Try All) $E \vdash \langle \ell \mapsto \mathtt{try}\ \imath\ \mathtt{All} \rangle : \star$ implies $E \vdash \ell : \mathtt{loc}\ \mathtt{a}(\mathtt{All})$, $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n)$ and $\mathtt{All} : () \to \mathtt{All}$. By (Red Try All) $\langle \ell \mapsto \mathtt{try}\ \imath\ \mathtt{All} \rangle \to \langle \ell \mapsto \mathtt{ok}\ \imath \rangle$ and $E \vdash \langle \ell \mapsto \mathtt{ok}\ \imath \rangle : \star$ because $E \vdash \imath_1 \dots \imath_n : A$ (for any A) and $A <: \mathtt{All}$, thus by (Type Sub) $E \vdash \imath_1 \dots \imath_n : \mathtt{All}$;

(Red Try Error) $E \vdash \prod_{k \in 1,\dots,n} \langle \imath_k \mapsto \mathtt{node}\ \mathtt{a_k}(v_k) \rangle \upharpoonright \langle \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n) \rangle \upharpoonright \langle \ell \mapsto \mathtt{try}\ \imath\ p(\vec{v}) \rangle : \star$ implies $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n)$, $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(v_k)$, $v_k = (\imath_{1_k} \dots \imath_{n_k})$ $E \vdash \ell : \mathtt{loc}\ \mathtt{a}(A)$, $p : (\vec{t}) \to A$, and $E \vdash \vec{v} : \vec{t}$. By the reduction $p(\vec{v}) := S$, thus $E \vdash S : A$. $\mathtt{a_1} \dots \mathtt{a_n} \not\vdash_S$, thus, by Proposition 13, $E \vdash \imath_1 \dots \imath_n : \overline{A}$ so, by (Type Let) and (Type Loc Fail), $E \vdash \langle \ell \mapsto \mathtt{fail}\ \imath \rangle : \star$;

(Red Test Ok) by rule (Type Loc Ok), (Type Loc Node), and (Type Test Loc) $E \vdash \langle \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n) \rangle \upharpoonright \prod_{k \in 1,\dots,n} \langle \jmath_k \mapsto \mathtt{ok}\ \imath_k \rangle \upharpoonright \langle \ell \mapsto \mathtt{test}\ \imath\ w \rangle : \star$ (where $w = \jmath_1 \dots \jmath_n$) implies $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n)$, $\forall k \in 1,\dots,n : E \vdash \jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)$, $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(u_k)$, and $E \vdash u_k : A_k$. Moreover $E \vdash \ell : \mathtt{loc}\ \mathtt{a}(A)$ and $\mathtt{a_1} \dots \mathtt{a_n} \vdash_A A_1 \dots A_n$.
$\mathtt{a_1} \dots \mathtt{a_n} \vdash_A A_1 \dots A_n$ implies $\mathtt{a_1}[A_1], \dots, \mathtt{a_n}[A_n] <: A$, by Proposition 9; thus by (Type Doc) $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(u_k)$, and $E \vdash u_k : A_k$ we have $E \vdash \imath_1 \dots \imath_n : \mathtt{a_1}[A_1], \dots, \mathtt{a_n}[A_n]$ and by (Type Sub) $E \vdash \imath_1 \dots \imath_n : A$. So by (Type Par) $E \vdash \langle \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n) \rangle \upharpoonright \prod_{k \in 1,\dots,n} \langle \jmath_k \mapsto \mathtt{ok}\ \imath_k \rangle \upharpoonright \langle \ell \mapsto \mathtt{ok}\ \imath \rangle : \star$;

(Red Test Fail) $E \vdash \langle \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n) \rangle \upharpoonright \prod_{k \in 1,\dots,n} \langle \jmath_k \mapsto d_k \rangle \upharpoonright \langle \ell \mapsto \mathtt{test}\ \imath\ w \rangle : \star$ (with $w = \jmath_1 \dots \jmath_n$) implies:

- by rule (Type Loc Node) $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n)$;
- by rule (Type Loc Ok) $\forall k \in 1,\dots,n$: s.t. $d_k = \mathtt{ok}\ \imath_k$ we have $E \vdash \jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)$, $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(v_k)$, and $E \vdash v_k : A_k$;
- by rule (Type Loc Fail) $\forall k \in 1,\dots,n$: s.t. $d_k = \mathtt{fail}\ \imath_k$ we have $E \vdash \jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)$, $E \vdash \imath_k : \mathtt{node}\ \mathtt{a_k}(v_k)$, and $E \vdash v_k : \overline{A_k}$;
- by rule (Type Test Loc) $E \vdash \ell : \mathtt{loc}\ \mathtt{a}(A)$, $E \vdash \imath : \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n)$, $E \vdash \jmath_k : \mathtt{loc}\ \mathtt{a_k}(A_k)$, $\mathtt{a_1} \dots \mathtt{a_n} \vdash_A A_1 \dots A_n$.

By (Red Test Fail) $\langle \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n) \rangle \upharpoonright \prod_{k \in 1,\dots,n} \langle \jmath_k \mapsto d_k \rangle \upharpoonright \langle \ell \mapsto \mathtt{test}\ \imath\ w \rangle \to \langle \imath \mapsto \mathtt{node}\ \mathtt{a}(\imath_1 \dots \imath_n) \rangle \upharpoonright \prod_{k \in 1,\dots,n} \langle \jmath_k \mapsto d_k \rangle \upharpoonright \langle \ell \mapsto \mathtt{fail}\ \imath \rangle$ if $\exists j \in$

$1, \ldots, n$: $\langle \jmath_j \mapsto \texttt{fail}\, \imath_j \rangle$ (note that for j we have $E \vdash v_j : \overline{A_j}$). Obviously $A \neq$ `All`, so by Proposition 10 $\mathtt{a_1}[A_1], \ldots, \mathtt{a_j}[\overline{A_j}], \ldots, \mathtt{a_n}[A_n] <: \overline{A}$. By rule (Type Doc) $E \vdash \imath_1 \ldots \imath_n : \mathtt{a_1}[A_1], \ldots, \mathtt{a_j}[\overline{A_j}], \ldots, \mathtt{a_n}[A_n]$ and by (Type Sub) $E \vdash \imath_1 \ldots \imath_n : \overline{A}$. In conclusion, by (Type Loc Fail), $E \vdash \langle \ell \mapsto \texttt{fail}\, \imath \rangle : \star$;

(Red Wait Ok) by rules (Type Par), (Type Loc Ok), (Type Wait), and (Type Loc Node) $E \vdash \langle \ell \mapsto \texttt{ok}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright \texttt{wait}\ \ell(x)\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t$ implies $u = \imath_1 \ldots \imath_n$, $E \vdash \imath : \texttt{node}\ \mathsf{a}(u)$, $E \vdash \ell : \texttt{loc}\ \mathsf{a}(A)$, $E \vdash u : A$, $E, x{:}A \vdash e_1 : t$, and $E, x{:}\overline{A} \vdash e_2 : t$. By rule (Red Wait Ok) $\langle \ell \mapsto \texttt{ok}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright \texttt{wait}\ \ell(x)\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \rightarrow \langle \ell \mapsto \texttt{ok}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright e_1\{x \leftarrow u\}$. By Proposition 5 (substitution), $E \vdash u : A$ and $E, x{:}A \vdash e_1 : t$ imply $E \vdash e_1\{x \leftarrow u\} : t$. Finally, by rule (Type Par), $E \vdash \langle \ell \mapsto \texttt{ok}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright e_1\{x \leftarrow u\} : t$;

(Red Wait Fail) by rules (Type Par), (Type Loc Fail), (Type Wait), and (Type Loc Node) $E \vdash \langle \ell \mapsto \texttt{fail}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright \texttt{wait}\ \ell(x)\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t$ implies $u = \imath_1 \ldots \imath_n$, $E \vdash \imath : \texttt{node}\ \mathsf{a}(u)$, $E \vdash \ell : \texttt{loc}\ \mathsf{a}(A)$, $E \vdash u : \overline{A}$, $E, x{:}A \vdash e_1 : t$, and $E, x{:}\overline{A} \vdash e_2 : t$. By rule (Red Wait Fail) $\langle \ell \mapsto \texttt{fail}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright \texttt{wait}\ \ell(x)\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \rightarrow \langle \ell \mapsto \texttt{fail}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright e_2\{x \leftarrow u\}$. By Proposition 5 (substitution), $E \vdash u : \overline{A}$ and $E, x{:}\overline{A} \vdash e_2 : t$ imply $E \vdash e_2\{x \leftarrow u\} : t$. Finally by rule (Type Par), $E \vdash \langle \ell \mapsto \texttt{fail}\, \imath \rangle \upharpoonright \langle \imath \mapsto \texttt{node}\, \mathsf{a}(u) \rangle \upharpoonright e_2\{x \leftarrow u\} : t$.

$\square$