A Theory of Contracts for Web Services

G. CASTAGNA; N. GESBERT; L. PADOVANI
A Theory of Contracts for Web Services
ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS (2009) 31(5)
DOI: 10.1145/1538917.1538920

A Theory of Contracts for Web Services

Giuseppe Castagna
CNRS PPS, Université Denis Diderot, Paris, France
and
Nils Gesbert
University of Glasgow, Glasgow, Scotland
and
Luca Padovani
ISTI, Università degli Studi di Urbino, Urbino, Italy

Contracts are behavioral descriptions of Web services. We devise a theory of contracts that formalizes the compatibility of a client to a service, and the safe replacement of a service with another service. The use of contracts statically ensures the successful completion of every possible interaction between compatible clients and services.

The technical device that underlies the theory is the *filter*, which is an explicit coercion preventing some possible behaviors of services and, in doing so, make services compatible with different usage scenarios. We show that filters can be seen as proofs of a sound and complete subcontracting deduction system which simultaneously refines and extends Hennessy's classical axiomatization of the must testing preorder. The relation is decidable and the decision algorithm is obtained via a cut-elimination process that proves the coherence of subcontracting as a logical system.

Despite the richness of the technical development, the resulting approach is based on simple ideas and basic intuitions. Remarkably, its application is mostly independent of the language used to program the services or the clients. We outline the practical aspects of our theory by studying two different concrete syntaxes for contracts and applying each of them to Web services languages. We also explore implementation issues of filters and discuss the perspectives of future research this work opens.

Categories and Subject Descriptors: F.1.2 [**Computation by Abstract Devices**]: Modes of Computation—*Parallelism and concurrency*; F.3.3 [**Logics and Meanings of Programs**]: Studies of Program Constructs—*Type structure*; H.3.5 [**Information Storage and Retrieval**]: Online Information Services—*Web-based services*; H.5.3 [**Information Interfaces and Presentation**]: Group and Organization Interfaces—*Theory and models, Web-based interaction*

General Terms: Languages, Standardization, Theory

Additional Key Words and Phrases: Web services, contracts, concurrency theory, ccs, must testing, type theory, subtyping, explicit coercions.

A preliminary version of this work appeared in the proceedings of POPL '08, the ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages 2008.
Nils Gesbert is supported by EPSRC grant EP/F065708/1 (Engineering Foundations of Web Services: Theories and Tool Support).

1. INTRODUCTION

Web services are distributed components that clients can connect to and communicate with by means of standard communication protocols and platform-neutral message formats. Remarkably, Web services are equipped with machine-understandable descriptions of their interface. This aspect permits Web services to be discovered according to the information encoded in their interface. Among the capabilities that can be used as search keys are the operations provided by the service, the format or *schema* [Fallside and Walmsley 2004] of the exchanged messages, and the *contract* required to interact successfully with the service. By contract we mean the description of the external, observable behavior of a service.

The Web Service Description Language (wsdl) [Chinnici et al. 2007; Chinnici et al. 2007] is a standard technology for describing the interface exposed by a service. In wsdl, contracts are basically limited to one-way (asynchronous) and request/response (synchronous) interactions. The Web Service Conversation Language (wscl) [Banerji et al. 2002] extends wsdl contracts by allowing the description of arbitrary, possibly cyclic sequences of exchanged messages between communicating parties. Other languages, such as the Web Service Business Execution Language (ws-bpel) [Alves et al. 2007], provide even more detailed descriptions of services by defining the subprocess structure and more specific details regarding the service's internals. Such descriptions, which are excessively concrete and verbose to directly serve as interfaces, can be approximated and compared in terms of contracts.

Standard technologies are also available for building repositories of Web service descriptions [Bellwood et al. 2005], making it possible to perform queries for services according to their contract. Searching immediately calls for a notion of contract equivalence to perform service discovery in the same way as, say, type isomorphisms are used to perform library searches [Rittri 1993; Di Cosmo 1995]. Without a formal characterization of contracts, however, one is left with excessively demanding equivalences such as syntactical or structural equality. In fact, clients will be equally satisfied to interact with services that provide *more* capabilities than those actually required, so that it makes sense to relax the equivalence into a *subcontract preorder* (denoted by $\preceq$ in this paper).

In this work we develop a formal theory of contracts that defines a coarse subcontract preorder. Along the lines of [Carpineti et al. 2006] we describe contracts by simple ccs-like terms built with just three operators: prefixing, denoted by a dot, and two infix choice operators $+$ (external choice) and $\oplus$ (internal choice). The contract $\alpha.\sigma$ describes a service that is capable of performing an action α, and then continues as σ. The contract $\sigma + \tau$ describes a service that lets the client decide whether to continue as σ or as τ. The contract $\sigma \oplus \tau$ describes a service that internally decides whether to continue as σ or as τ. Following ccs notation, actions are either write or read actions, the former ones being topped by a bar, and one being the *co-action* of the other. Actions can either represent *operations* or *message types*. As a matter of facts, contracts are behavioral types of processes that do not manifest internal moves and the parallel structure.

Contracts are used to ensure that interactions between clients and services will always succeed. Intuitively, this happens if whenever a service offers some set of

actions, the client either synchronizes with one of them (that is, it performs the corresponding co-action) or it terminates. The service contract allows us to determine the set of clients that *comply* with it, that is that will successfully terminate any session of interaction with the service.

Of course the client will probably be satisfied to interact with services that offer more than what the searched contract specifies. Intuitively we want to define an order relation on contracts $\sigma \leq \tau$ such that every client complying with services implementing σ will also comply with services of contract τ. In particular, we would like the $\leq$ preorder to enjoy some basic properties. The first one is that it should be safe to replace (the service exposing) a contract with a "more deterministic" one. For instance, we expect $\bar{a} \oplus \bar{b}.c \leq \bar{a}$, since every client that terminates with a service that may offer either $\bar{a}$ or $\bar{b}.c$ will also terminate with a service that systematically offers $\bar{a}$. The second desirable property is that it should be safe to replace (the service exposing) a contract with another one that offers more capabilities. For instance, we expect $\bar{a} \leq \bar{a} + \bar{b}.d$ since a client that terminates with services that implement $\bar{a}$ will also terminate with services that leave the client the choice between $\bar{a}$ and $\bar{b}.d$. If taken together, these two examples show the main problem of this intuition: it is easy to see that a client that complies with $\bar{a} \oplus \bar{b}.c$ does not necessarily comply with $\bar{a} + \bar{b}.d$: if client and service synchronize on b, then the client will try to write on c while the service expects to read from d. Therefore, under this interpretation, $\leq$ looks as not being transitive:

$$\bar{a} \oplus \bar{b}.c \leq \bar{a} \quad \wedge \quad \bar{a} \leq \bar{a} + \bar{b}.d \quad \Longrightarrow \quad \bar{a} \oplus \bar{b}.c \leq \bar{a} + \bar{b}.d\,.$$

The problem can be solved by resorting to the theory of *explicit coercions* [Bruce and Longo 1990; Chen 2004; Soloviev et al. 1996]. The flawed assumption of the approach described so far, which is the one proposed in [Carpineti et al. 2006], is that services are used carelessly "as they are". Note indeed that what we are doing here is to use a service of "type" $\bar{a} + \bar{b}.d$ where a service of type $\bar{a} \oplus \bar{b}.c$ is expected. The knowledgeable reader will have recognized that we are using $\leq$ as an *inverse* subtyping relation for services.[1] If we denote by $:>$ the subtyping relation for services, then $\bar{a} \oplus \bar{b}.c \;:>\; \bar{a} + \bar{b}.d$ and so what we implicitly did is to apply subsumption [Cardelli 1988] and consider that a service that has type $\bar{a} + \bar{b}.d$ has also type $\bar{a} \oplus \bar{b}.c$. The problem is not that $\leq$ (or, equivalently, $:>$) is not transitive. It rather resides in the use of subsumption, since this corresponds to the use of *implicit* coercions. Coercions have many distinct characterizations in the literature, but they all share the same underlying intuition that coercions are functions that embed objects of a smaller type into a larger type "without adding new computation" [Chen 2004]. For instance it is well known that for record types one has $\{a{:}s\} :> \{a{:}s; b{:}t\}$. This is so because the coercion function $c = \lambda x^{\{a:s;b:t\}}.\{a = x.a\}$ embeds values of the smaller type into the larger one.[2]

[1] The inversion is due to the fact that we are considering the client perspective: a contract can be interpreted as the set of clients that comply with services implementing the contract. We decided to keep this notation rather than the inverse one for historical reasons, since it is the same sense as used by De Nicola and Hennessy for the may and must preorders [De Nicola and Hennessy 1984]. This inversion corresponds to the duality between simulation and subtyping, viz. between observers and observed behaviors.

[2] In typed lambda calculus coercions are formally characterized by the fact that their type erasure

In order to use a term of type $\{a{:}s; b{:}t\}$ where one of type $\{a{:}s\}$ is expected, we first have to embed it in the right type by the coercion function c above, which erases (masks/shields) the b field so that it cannot interfere with the computation. Most programming languages do not require the programmer to write coercions, either because they do not have any actual effect (as in the case of the function c above since the type system already ensures that the b field will never be used) or because they are inserted by the compiler (as when converting an integer into the corresponding float). In this case we speak of *implicit* coercions. However some programming languages (e.g. OCaml [OCaml]) resort to *explicit* coercions because they have a visible effect and, for instance, they cannot be inferred by the compiler.

Coercions for contracts have an observable effect, therefore we develop their metatheory in terms of explicit coercions. However, coercions can be inferred so they can be kept implicit in the language and automatically computed at static time. Coming back to our example, the embedding of a service of type $\neg a$ into $\neg a \oplus \neg b.c$ is the identity, since we do not have to mask/shield any action of a service of the former type in order to use it in a context where a service of the latter type is expected. On the contrary, to embed a service of type $\neg a + \neg b.d$ into $\neg a$ we have to mask (at least) the $\neg b$ action of the service. In order to use it in a context that expects a $\neg a$ service we apply to it a *filter* that will block all $\neg b$ messages. Transitivity being a logical cut, the coercion from $\neg a + \neg b.d$ to $\neg a \oplus \neg b.c$ is the composition of the two coercions, that is the filter that blocks $\neg b$ messages. So if we have a client that complies with $\neg a \oplus \neg b.c$, then it can be used with a service that implements $\neg a + \neg b.d$ by applying to this service the filter that blocks its $\neg b$ messages. This filter will make the previous problematic synchronization on b impossible, so the client can do nothing but terminate.

Filters thus reconcile two requirements that were hitherto incompatible: On the one hand we wish to replace an old service by a new service that offers more choices (that is *width subtyping*, e.g. $\sigma :> \sigma + \tau$) and/or longer interaction patterns (that is *depth subtyping*, e.g. $a :> a.\sigma$) and/or is more deterministic (e.g. $\sigma \oplus \tau :> \sigma$). On the other hand we want clients of the old service to seamlessly work with the new one.

Two observations to conclude this brief overview. First, the fact that we apply filters to services rather than to clients is just a presentational convenience: the same effect can be obtained by applying to the client the filter that blocks the corresponding co-actions. Second, filters must be finer-grained in blocking actions than restriction operators as defined for ccs or π. These are "permanent" blocks, while filters are required to be able to modulate blocks along the computation. For instance the filter that embeds $(a.(a + b)) + b.c$ into $a.b$ must block b only at the first step of the interaction and a only at the second step of the interaction.

1.1 Outline of the presentation

We start by presenting the syntax of our contracts (§2.1), by showing how to use them to express wsdl and wscl descriptions (§2.2), and by defining their semantics (§2.3). We then characterize the set of all clients that are strongly compliant with a service—that is, clients that successfully complete every direct interaction

---

is η-equivalent to the identity function, but in general coercions may be different from the identity function [Chen 2004].

session with the service—and argue that subcontract relations whose definitions are naively based on strong compliance are either too strict or suffer the aforementioned problem of transitivity (§2.4). We argue that subcontracting should not be defined on all possible interactions, but focus only on interactions based on actions that a client expects from the services: all the other possible actions should not interfere with the interaction. We formalize this concept by giving a coinductive definition of a subcontract relation that focuses on this kind of actions, we study its properties and describe the relation with the must preorder (§3.1). This subcontract relation induces a notion of weak compliance suggesting that non-interference of unexpected actions can be ensured by coercion functions, which we dub *filters* (§3.2). By shielding the actions at issue, a filter embeds a service into the "world" of its expected clients. We prove that our subcontract relation can be expressed in terms of filters and of the must preorder and we provide a sound and complete deduction system for the subcontract relation where filters play the role of "proofs" (§3.3). The subcontract relation is shown to be decidable via the definition of a sound and complete algorithmic deduction system (§3.4). Next we show how our contracts are to be used to type Web services programming languages. In particular, we relate our contract language with a generic class of typed process languages and show the soundness of our theory of contracts: this is proved by showing that if a client process is weakly compliant with a service process via a given filter, then the filter ensures that the client will either synchronize infinitely many times with the service or it will successfully terminate (§4). We conclude by exploring the more practical aspects of this work. In particular, since our theory is stated for possibly infinite regular trees, we introduce two concrete syntaxes to finitely denote these trees and relate them with the preceding theoretical work (§5.1). Next we apply each syntax to one language proposed by the two major web standardization bodies (i.e., w3c and Oasis) (§5.2-5.3), we explore possible ways of implementing filters, and we outline how the theory can be directly implemented in ws-bpel without requiring any modification of the ws-bpel specification or of existing ws-bpel processes (§5.4). A conclusion recaps our work and hints at possible tracks of future research (§6).

1.2 Related work

The contracts used in this presentation draw their inspiration from De Nicola and Hennessy's seminal work "ccs without τ's" [De Nicola and Hennessy 1987], as well as from acceptance trees [Hennessy 1985; 1988] of which they can be considered an alternative representation. The works that are most closely related to ours are by Carpineti et al. [2006] and those on *session types*, especially the one by Gay and Hole [2005]. In [Carpineti et al. 2006] the subcontract relation exhibits all the desirable properties illustrated in the introduction, but subcontracting stops at the problem of transitivity. In that work compliance was a syntactic notion and contracts lacked a semantic characterization.

Session types were introduced in the context of the π-calculus [Honda 1993; Takeuchi et al. 1994; Honda et al. 1998]. These are used to type special channels through which several different messages may be exchanged in sequence according to a given protocol. Such a session channel can be seen as a client-service connection, and the session type is the analogous of our contract as it describes which actions

the processes may perform through this channel. However, session types have the important restriction, if compared with contracts, that only one part has the floor at a given time: whenever a process performs an internal choice it has to indicate explicitly which path of interaction it has chosen, and the other process has to be waiting for this indication. Thus there is no way of mixing internal and external choices, and two processes like $a + b$ and $\overline{a} + \overline{b}$ do not interact successfully (because nobody has the floor, so no communication can happen). Subtyping for the session types has been studied by Gay and Hole [2005], but because of the aforementioned restriction, the transitivity problem we address in this paper does not exist for them: internal and external choices can never be related, hence $a \oplus b \not\leq a + b$ does *not* hold. However, this looks like a reasonable relation, inasmuch as $a \oplus b$ models a scenario where exactly one of two resources a and b is available (and the client does not know *which* one), which can be safely related with (and replaced by) a scenario where both a and b are available and the client can choose whether to use a or b.

[Carbone et al. 2007a; 2007b] describe choreographies of Web services by means of a global calculus, and descriptions of individual processes are obtained as projections of the global description. Both the global description and the projections are based on session types. In our approach, the typical application is searching for a service compatible with a given protocol *from the client's point of view*: in particular, we want depth subtyping (a service that tries to pursue the interaction after the client has successfully terminated is compatible with this client), which does not hold for session types. We believe that our theory is more basic than the theory of session types and that it can be fruitfully used to enrich the latter.

[Fournet et al. 2004] define a *conformance* preorder on ccs processes with the property that a process is *stuck-free* (i.e., it successfully terminates) in every context in which smaller processes are stuck-free. The *conformance* relation of [Fournet et al. 2004] differs from our subcontract relation in some important aspects. For example, in [Fournet et al. 2004] $a \oplus \mathbf{0} \not\leq \mathbf{0}$, but $a \oplus \mathbf{0} \;;\not\leq a$. This essentially derives from the fact that stuck-free conformance is defined without using an explicit action (denoted by e in our work) expressing in an observationally visible way the successful termination of a party, but instead by requiring that the party must eventually reduce to the idle process $\mathbf{0}$. Doing so prevents the specification of clients of the form $e + \overline{a}.e$, which *attempt* to do an action, but that can succeed even if the action is not available. The lack of the explicit action e has overall important consequences on the precongruence properties of $\not\leq$. A more important point is that the conformance relation of Fournet et al. is not complete with respect to stuck-freedom, in the sense that there are processes that are stuck-free exactly in the same contexts but are not related by conformance: for instance, $a.(b \oplus c)$ and $a.b + a.c$ are stuck-free equivalent but are not conformance equivalent. In our theory the two processes above are equivalent and, more generally, our subcontracting provides, *mutatis mutandis* (*cf.* actions for successful termination), a complete characterization of stuck-freedom. Finally, stuck-freedom does not allow either width or depth subtyping.

[Bravetti and Zavattaro 2007] propose a contract language equipped with a refinement relation. The language is constrained so that output actions can only

occur in the context of an internal choice. This restriction somehow resembles the design choice of session types and, not surprisingly, the refinement relation for this language allows width extensions of contracts without any intervening filtering. However, the refinement relation is determined in a symmetric way for all the participants of a system, whereas our notion of compliance is asymmetric (in favor of the client). This makes the refinement relation more demanding than ours. In particular, all the participants must successfully terminate, meaning that depth extensions are not entailed by refinement.

[Derrick et al. 1996] provides a thorough overview of refinement relations in the testing framework that date back to the LOTOS system [Brinksma et al. 1995]. According to the terminology of [Derrick et al. 1996], the relation $\bar{a} \oplus \bar{b}.c \leq \bar{a}$ is an instance of so-called *reduction refinement*, in which $\bar{a} \oplus \bar{b}.c$ is replaced by $\bar{a}$ thus reducing nondeterminism. On the other hand, $\bar{a} \leq \bar{a} + \bar{b}.d$ is an instance of so-called *extension refinement*, in which a $\bar{a}$ is replaced by $\bar{a} + \bar{b}.d$ which provides further functionalities. The combination of these two refinement relations yields the so-called *implementation refinement*, which basically coincides both with the subcontract relation defined in [Carpineti et al. 2006] and with the $\leq$ relation we introduce in this work (see equation (1) in §2.3 and the proof of Theorem 3.4). It is known that extension refinement is not a precongruence with respect to the contract operators and that implementation refinement lacks transitivity [Derrick et al. 1996]. As we already explained in the Introduction, the present paper addresses and solves both problems: precongruence can be regained under minimal conditions, namely when filtering does not depend on the internal choices of client and service (see §3.3), and transitivity stems directly from the ability of composing filters.

A very preliminary version of this work was presented at Plan-X 2007 workshop [Castagna et al. 2007] and largely improved in the version presented one year later at Popl '08 [Castagna et al. 2008]. Although the Plan-X workshop has just informal proceedings, these are available on the web. Therefore it seems worth discussing the differences of the present article both with the Plan-X version and with the improved Popl version. While the overall presentation and structure of the three papers is the same, both this and the Popl versions improve over the Plan-X one in several points. Here and in [Castagna et al. 2008] we consider a slightly different version of strong compliance relation which now coincides with the must testing preorder, while in Plan-X strong compliance differed from must testing for some (uninteresting) pathological cases that involved the empty contract. The deduction system of Plan-X was reworked in favor of elegance and simplicity. The resulting algebraic theory of filters is also cleaner. We present better results for language neutrality. Finally, the study of the algorithmic version of the deduction system, of its logical interpretation, and of the decidability of the containment relation, was absent from the Plan-X version and introduced in the Popl one. The article presented here improves the work in Popl for several key aspects. Foremost, while in Popl work contracts (and filters) were finite, here the theory is defined for recursive contracts (and filters) by working directly with infinite recursive trees and by proposing two different finite representations for them (we believe that the in-depth treatment of infinite terms and of the relation with their finite representations constitutes a nice contribution of our work). This im-

plied a complete reworking of most of the definitions and of the proofs (even though the latter were not included in the Popl proceedings for space reasons). The finite representations we introduce here are then used to study wscl and ws-bpel and possible implementations of filters are explored; in particular we outline how our theory can be used and implemented in the current specification of ws-bpel without requiring any modification to the language or to existing ws-bpel processes. All these practical aspects are completely absent in the work presented at Popl. Finally, the deduction system for filters is here further improved and we also use a different and (we hope) more elegant syntax for filters, by relying only on the underlying algebraic operators.

Starting from the Plan-X work the third author and Cosimo Laneve proposed a simplification where contracts are "statically" filtered [Laneve and Padovani 2007]: each contract is associated with a *static interface* (in the sense that it does not change over the time) declaring the only visible actions of the contract and blocking all the other ones whenever they happen. As stated in [Laneve and Padovani 2007], the resulting approach is less general than ours and, consequently, yields a stricter subcontract relation. For instance, the relation $a.b \not\leq (a.(a + b)) + b.c$, which we commented on just before §1.1, does not hold in the interface approach (for a practical example of relation that does not hold for interfaces see the contracts σ and σ' in §2.2.2 and the explanation given at the end of §3.2.1). On the other hand, interfaces allow for simpler algorithmic treatment and implementation.

2. CONTRACTS

2.1 Syntax

Contracts are formally defined as possibly infinite trees that satisfy regularity and a contractivity condition.

Definition 2.1 (contract). *Let N be a countable set of names. The set of contracts Σ is the set of possibly infinite terms coinductively generated by the following grammar:*

$$\begin{array}{lll} \alpha & ::= & a \mid \overline{a} \qquad\qquad a \in N \\ \sigma & ::= & \mathbf{0} \mid \alpha.\sigma \mid \sigma \oplus \sigma \mid \sigma + \sigma \end{array}$$

and satisfying the following conditions:

(1) *contract terms are regular,*

(2) *on every infinite branch of a contract term there are infinitely many occurrences of the prefix constructor.*

In the definition **0** is the contract of services that do not perform any action while the other constructions were already explained in the introduction. We follow the standard convention of omitting trailing **0**'s. We also work modulo associativity of each sum operator and by an abuse of notation we will sometimes denote them as n-ary operators. We then write $\sum_{i\in\{1,\dots,n\}} \sigma_i$ for $\sigma_1 + \sigma_2 + \cdots + \sigma_n$ and $\bigoplus_{i\in\{1,\dots,n\}} \sigma_i$ for $\sigma_1 \oplus \sigma_2 \oplus \cdots \oplus \sigma_n$. By convention we have $\sum_{i\in\emptyset} \sigma_i = \mathbf{0}$.

Infinite terms account for recursive contracts. This kind of presentation is not customary in process calculi where finite representations of recursion (essentially, Kleene star, recursive equations, or rec-notations) are nearly always preferred. This

is probably due to the fact that the intuition behind a finite representation can be more easily grasped. However working directly on infinite trees has two clear advantages. First and foremost all results abstract away from the particular notation used to represent recursion: it is easy to transpose each result to each particular representation, while it is much more difficult to move from one representation to another. Second, working with infinite terms makes it quite straightforward to transpose the work to finite ones since it just suffices to forget that terms are infinite and no further modifications are needed; with finite representations of recursion, instead, definitions and results must be tailored to account for infinite behavior and thus use constructions (such as environments for recursion variables, memoization environments in deductions) that are meaningless for finite terms.

Of course not every infinite term constructed by applying "$\oplus$", "$+$", and "$\cdot$" is acceptable. We require the term (*i*) to be regular, so that the set of terms is provided with a well-founded order, and (*ii*) to satisfy a fairly standard contractivity condition requiring that recursion must be guarded by an i/o operation, which rules out meaningless terms of the form $\mathrm{rec}\ x = x + x$.[3]

2.2 Examples

In this section we relate our contract language to existing technologies for specifying service protocols.

2.2.1 *Message exchange patterns in* wsdl. The Web Service Description Language [Chinnici et al. 2007; Chinnici et al. 2007] permits to describe and publish abstract and concrete descriptions of Web services. Such descriptions include the schema of messages exchanged between client and server, the name and type of *operations* that the service exposes, as well as the locations (urls) where the service can be contacted. In addition, it defines interaction patterns (called *message exchange patterns* or meps in version 2.0 of wsdl) determining the order and direction of the exchanged messages. In particular, wsdl 2.0 predefines four message exchange patterns for describing services where the interaction is initiated by clients. Let us shortly discuss how the informal plain English semantics of these patterns can be formally defined in our contract language. When the mep is inOnly or robustInOnly, communication is basically *asynchronous*: the client can only send an In message containing the request. If the pattern is robustInOnly the service may optionally send back a Fault message indicating that an error has occurred. When the mep is inOut or inOptOut, communication is basically *synchronous*: the client sends an In message containing the request and the service sends back either an Out message containing the response or a Fault message. If the pattern is inOptOut, then the Out message is optional. These four patterns can be encoded

[3] Contractivity was introduced by Courcelle [Courcelle 1983] to rule out e.g. $\mathrm{rec}\ x = x$, which is *syntactically* meaningless because it is satisfied by every regular tree, but it was not meant to rule out expressions such as $\mathrm{rec}\ x = x + x$. The latter is syntactically meaningful since it denotes a particular regular tree, but it is *semantically* meaningless, because of the the peculiar semantics of the "$+$" operator. Here we use *contractivity* in stricter interpretation, that is as a means for ruling out also terms that are *semantically* meaningless.

in our contract language as follows:

$$\begin{aligned} \text{inOnly} &= \text{In} \\ \text{robustInOnly} &= \text{In}.(\mathbf{0} \oplus \overline{\text{Fault}}) \\ \text{inOut} &= \text{In}.(\overline{\text{Out}} \oplus \overline{\text{Fault}}) \\ \text{inOptOut} &= \text{In}.(\mathbf{0} \oplus \overline{\text{Out}} \oplus \overline{\text{Fault}}) \end{aligned}$$

Intuitively, a client that is capable of invoking a service whose mep is inOnly will also interact successfully with a service whose mep is robustInOnly (depth subtyping). Conversely, a client that is capable of invoking a service whose mep inOptOut will also interact successfully with services whose mep is either inOut, or robustInOnly (since they are more deterministic), or even inOnly. Indeed, such a client must be able to handle *both* a communication that terminates *and* a Fault or Out message. On the other hand, a client that interacts with a service whose mep is inOut will not (always) interact successfully with a service whose mep is inOptOut. The client assumes that it will always receive either an Out or a Fault message, but inOptOut does not give this guarantee.

2.2.2 *Conversations in* wscl. The wsdl message exchange patterns cover only the simplest forms of interaction between a client and a service. More involved forms of interactions, in particular stateful interactions, cannot be captured if not as informal annotations within the wsdl interface. The Web service conversation language wscl [Banerji et al. 2002] provides a more general specification language for describing complex *conversations* between two communicating parties, by means of an activity diagram (Figure 1). The diagram is made of *interactions* which are connected with each other by means of *transitions*. An interaction is a basic one-way or two-way communication between the client and the server. Two-way communications are just a shorthand for two sequential one-way interactions. Each interaction has a *name* and a list of *document types* that can be exchanged during its execution. A transition connects a *source* interaction with a *destination* interaction. A transition may be *labeled* by a document type if it is active only when a message of that specific document type was exchanged during the previous interaction.

Below we encode the contract of a simplified e-commerce service (Figure 1) where the client is required to login before it can select and buy items from the store. If the login is successful, the client can issue one or more queries and add items to the shopping cart. The client can buy the items in the shopping cart using one of two payment methods, either with credit card or with a bank transfer. At any time, the client can choose to logout and leave the store. In case of purchase, the service reports whether the purchase was valid. We can represent the contract of Figure 1 (without the dashed part, which represents an extension discussed later), as the regular contract σ_1 defined by the equations:

$$\sigma_1 \stackrel{\text{def}}{=} \text{Login}.(\overline{\text{InvalidLogin}} \oplus \overline{\text{ValidLogin}}.\sigma_2)$$

$$\sigma_2 \stackrel{\text{def}}{=} \text{Query}.\overline{\text{Catalog}}.(\sigma_2 + \text{Logout} + \text{AddToCart}.(\sigma_2 + \text{Buy}.\sigma_3))$$

$$\sigma_3 \stackrel{\text{def}}{=} \text{Logout} + \text{CreditCard}.(\overline{\text{Valid}} \oplus \overline{\text{Invalid}}) + \text{BankTransfer}.(\overline{\text{Valid}} \oplus \overline{\text{Invalid}})$$

Unlabeled transitions in Figure 1 correspond to external choices in the contract, whereas labeled transitions correspond to internal choices. The use of recursion in the definition of σ_2, corresponds to the presence of (two) cycles in the wscl graph.

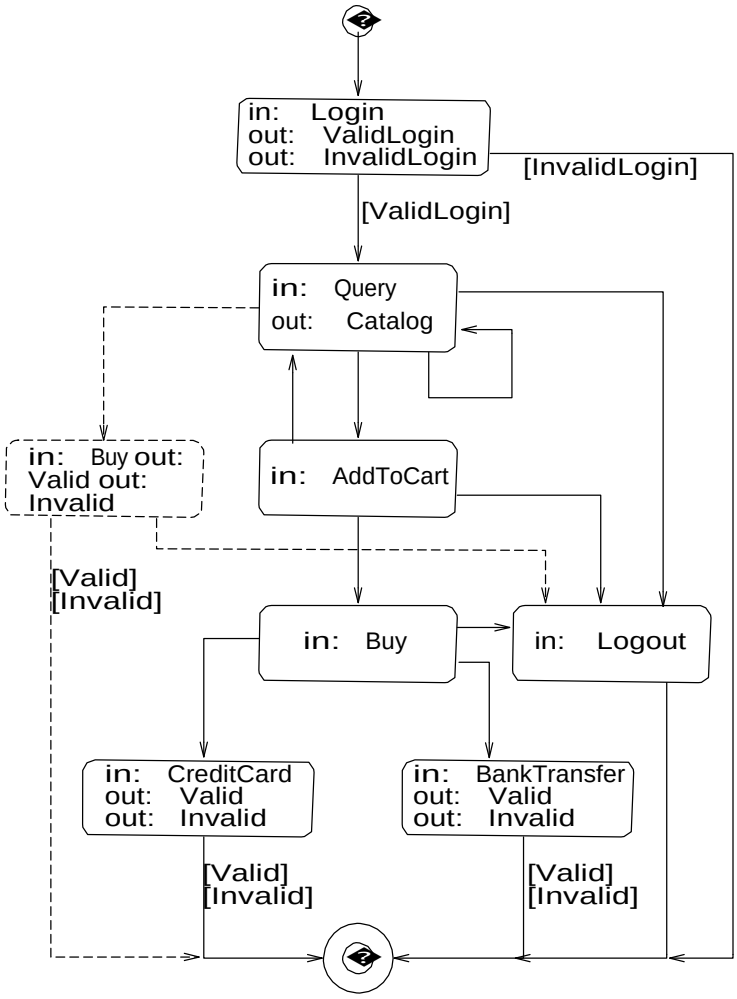

Fig. 1. Contract of an e-commerce service as a wscl diagram.

Let us recast in this setting the three forms of subtyping we described in the introduction. First, it is clear that clients compliant with the service above will always be happy with more deterministic servers that, for instance, never deny the access ($\overline{\text{InvalidLogin}} \oplus \overline{\text{ValidLogin}} \,\&\, \overline{\text{ValidLogin}}$) as well as with servers that offer longer interactions, such as the fact of proposing an invoice after the payment ($\overline{\text{Valid}} \,\&\, \overline{\text{Valid.Invoice}}$). Now assume that the service is extended (by width subtyping) with "1-click ordering" capability, so that if the client has already bought items, perhaps in some previous sessions, it is allowed to buy further items without adding them to the shopping cart, and without the need to re-send the payment information (dashed part in Figure 1). The contract σ_2 would change to

σ_2' as follows:

$$\sigma_2' \stackrel{\text{def}}{=} \text{Query}.\overline{\text{Catalog}}.(\sigma_2' + \text{Logout} + \text{AddToCart}.(\sigma_2' + \text{Buy}.\sigma_3) + \sigma_4)$$
$$\sigma_4 \stackrel{\text{def}}{=} \text{Buy}.(\overline{\text{Valid}} \oplus \overline{\text{Invalid}})$$

It would be desirable for clients that are compliant with the former service to be compliant with this service as well. After all, the extended service offers *more* than the old one. However, the transitivity problem we pointed out in the introduction might arise. Indeed, assume to have a client that does actually account for a Buy message right after receiving a catalog from the service and that such a client is compliant with the former service for the simple reason that, since the former service did not provide a "1-click ordering" capability, whatever contract ρ_B the client provided after the Buy action was irrelevant to establish compliance. In the extended service this is no longer the case and, since the ρ_B may be incompatible with the continuation of σ_4 after Buy, the client can safely interact with the extended service only if the new Buy action is filtered out (see §3.2.1).

2.3 Semantics

Contracts describe the behavior of the processes that implement them. This behavior is determined by the actions that are offered by a process and the way in which they are offered (note that both $\sigma \oplus \tau$ and $\sigma + \tau$ offer the same actions). This is formally stated by the Definitions 2.2 and 2.4 given below.

Definition 2.2 (transition). *Let $\sigma \overset{\alpha}{\rightarrow}$ be the least relation such that:*

$$\mathbf{0} \not\overset{\alpha}{\rightarrow} \qquad \frac{\alpha := \beta}{\beta.\sigma \overset{\alpha}{\rightarrow}} \qquad \frac{\sigma \overset{\alpha}{\rightarrow} \quad \tau \not\overset{\alpha}{\rightarrow}}{\sigma \oplus \tau \overset{\alpha}{\rightarrow}} \qquad \frac{\sigma \overset{\alpha}{\rightarrow} \quad \tau \not\overset{\alpha}{\rightarrow}}{\sigma + \tau \overset{\alpha}{\rightarrow}}$$

The transition relation *of contracts, noted $\overset{\alpha}{\longrightarrow}$, is the least relation satisfying the rules:*

$$\alpha.\sigma \overset{\alpha}{\longrightarrow} \sigma$$

$$\frac{\sigma \overset{\alpha}{\longrightarrow} \sigma' \quad \tau \overset{\alpha}{\longrightarrow} \tau'}{\sigma + \tau \overset{\alpha}{\longrightarrow} \sigma' \oplus \tau'} \qquad \frac{\sigma \overset{\alpha}{\longrightarrow} \sigma' \quad \tau \not\overset{\alpha}{\rightarrow}}{\sigma + \tau \overset{\alpha}{\longrightarrow} \sigma'} \qquad \frac{\sigma \overset{\alpha}{\longrightarrow} \sigma' \quad \tau \overset{\alpha}{\longrightarrow} \tau'}{\sigma \oplus \tau \overset{\alpha}{\longrightarrow} \sigma' \oplus \tau'} \qquad \frac{\sigma \overset{\alpha}{\longrightarrow} \sigma' \quad \tau \not\overset{\alpha}{\rightarrow}}{\sigma \oplus \tau \overset{\alpha}{\longrightarrow} \sigma'}$$

and closed under mirror cases for the external and internal choices. We write $\sigma \overset{\alpha}{\longrightarrow}$ if there exists σ' such that $\sigma \overset{\alpha}{\longrightarrow} \sigma'$.

The relation $\overset{\alpha}{\longrightarrow}$ is different from standard transition relations for ccs processes [Milner 1982]. For example, there is always at most one contract σ' such that $\sigma \overset{\alpha}{\longrightarrow} \sigma'$, while this is not the case in ccs (the process $a.b + a.c$ has two different a-successor states: b and c). This mismatch is due to the fact that contract transitions define the evolution of conversation protocols *from the perspective of an external communicating party*. Thus $a.b + a.c \overset{a}{\longrightarrow} b \oplus c$ because, once the action a has been performed, the communicating party is not aware of which branch has been chosen. On the contrary, ccs transitions define the evolution of processes *from the perspective of the process itself*.

Notation 2.3. *We use* init(σ) *to denote the set of actions that can be immediately emitted by* σ*, that is* $\text{init}(\sigma) = \{\alpha \mid \sigma \xrightarrow{\alpha}\}$.

Let $\sigma \xrightarrow{\alpha}$. *We write* $\sigma(\alpha)$ *for the unique continuation of* σ *after* α*, that is, the contract* σ' *such that* $\sigma \xrightarrow{\alpha} \sigma'$. *We extend the notion of continuation to sequences of actions. Let* ϕ *denote a possibly empty, finite string of actions. If* $\phi = \varepsilon$*, then* $\sigma \xrightarrow{\phi} \sigma$ *and we have* $\sigma(\phi) = \sigma$*; if* $\phi = \alpha\phi'$*, then* $\sigma \xrightarrow{\phi} \sigma'$ *if* $\sigma \xrightarrow{\alpha} \sigma' \xrightarrow{\phi} \sigma''$ *and we have* $\sigma(\phi) = \sigma''$.

The labeled transition system above describes the actions offered by (a service implementing) a contract, but does not show *how* these actions are offered. In particular the actions offered by an external choice are all available at once while the actions offered by different components of an internal choice are mutually exclusive. Such a description is given by the *ready sets* that are observable for a given contract:

Definition 2.4 (observable ready sets). *Let* $\mathcal{P}_f(N \cup \overline{N})$ *be the set of finite parts of* $N \cup \overline{N}$*, called* ready sets*. Let also* $\sigma \Downarrow \mathbf{r}$ *be the least relation between contracts* σ *in* Σ *and ready sets* $\mathbf{r}$ *in* $\mathcal{P}_f(N \cup \overline{N})$ *such that:*

$$\mathbf{0} \Downarrow \emptyset \qquad \alpha.\sigma \Downarrow \{\alpha\} \qquad \frac{\sigma \Downarrow \mathbf{r} \quad \tau \Downarrow \mathbf{s}}{\sigma + \tau \Downarrow \mathbf{r} \cup \mathbf{s}} \qquad \frac{\sigma \Downarrow \mathbf{r}}{\sigma \oplus \tau \Downarrow \mathbf{r}} \qquad \frac{\tau \Downarrow \mathbf{r}}{\sigma \oplus \tau \Downarrow \mathbf{r}}$$

Notation 2.5. *We use the convention that the bar operation is an involution,* $\overline{\overline{a}} = a$*, and for a given ready set* $\mathbf{r}$ *we define its complementary ready set as* $\text{co}(\mathbf{r}) = \{\overline{\alpha} \mid \alpha \in \mathbf{r}\}$.

2.4 The problem

We now possess all the technical instruments to formally state the problem we described in the introduction and recalled at the end of §2.2. This first requires the precise definition of *compliance*. Recall that, intuitively, the behavior of a client complies with the behavior of a service if for every set of actions that the service may offer, the client either synchronizes with one of them, or it terminates successfully. The behavior of clients, as well as the one of services, is described by contracts. Therefore we need to define when a contract ρ describing the behavior of a client complies with a contract σ describing the behavior of a service. For this we reserve a special action e (for "end") that can occur in client contracts and that represents the ability of the client to successfully terminate. Then we require that, whenever no further interaction is possible between the client and the service, the client be in a state where this action is available.

Definition 2.6 (strong compliance). *C is a* strong compliance relation *if* $(\rho, \sigma) \in C$ *implies that:*

(*1*) $\rho \Downarrow \mathbf{r}$ *and* $\sigma \Downarrow \mathbf{s}$ *implies either* $\mathbf{e} \in \mathbf{r}$ *or* $\text{co}(\mathbf{r}) \cap \mathbf{s} \neq \emptyset$*, and*

(*2*) $\rho \xrightarrow{\overline{\alpha}} \rho'$ *and* $\sigma \xrightarrow{\alpha} \sigma'$ *implies* $(\rho', \sigma') \in C$.

We use $\asymp$ *to denote the largest strong compliance relation.*

In words the definition above states that a client of contract ρ is compliant with a service of contract σ if (1) for every possible combination s and $\mathbf{r}$ of the independent

choices of the service and the client, either there is an action in the client choice that can synchronize with an action among those offered by the service ($\mathrm{co}(\mathbf{r}) \cap \mathrm{s} \neq \emptyset$) or the client terminates successfully ($\mathrm{e} \in \mathbf{r}$), and (2) whenever a synchronization happens, the continuation of the client after it is compliant with the continuation of the service ($(\rho', \sigma') \in C$).

Once we have such a definition it is natural to define the subcontract relation in terms of compliance. Intuitively, (client) contracts are seen as "tests" for comparing (service) contracts. Two (service) contracts are related if so are the sets of (client) contracts compliant with them [De Nicola and Hennessy 1984].

Definition 2.7 (strong subcontract). *The contract σ is a* strong subcontract *of the contract τ, written $\sigma \subsetneq \tau$, if and only if for all ρ we have $\rho \dashv\vdash \sigma$ implies $\rho \dashv\vdash \tau$. We write $\sigma \simeq \tau$ if $\sigma \subsetneq \tau$ and $\tau \subsetneq \sigma$.*

This definition corresponds to giving a set theoretic semantics to service contracts which are thus interpreted as the set of their compliant clients. Thus $\subsetneq$ is interpreted as set-theoretic inclusion.

As usual with testing semantics, it is hard to establish a relationship between two contracts because the set of clients that are strongly compliant is infinite. A direct definition of the preorder is therefore preferred:

Definition 2.8 (coinductive strong subcontract). *$\mathcal{S}$ is a coinductive strong subcontract relation if $(\sigma, \tau) \in \mathcal{S}$ implies that*

(1) *$\tau \Downarrow \mathbf{r}$ implies that there exists $\mathrm{s} \subseteq \mathbf{r}$ such that $\sigma \Downarrow \mathrm{s}$, and*

(2) *$\tau \xrightarrow{\alpha} \tau'$ implies $\sigma \xrightarrow{\alpha} \sigma'$ and $(\sigma', \tau') \in \mathcal{S}$.*

Theorem 2.9. *$\subsetneq$ is the largest coinductive strong subcontract relation.*

Proof. First of all we prove that $\subsetneq$ is a coinductive subcontract relation. Assume $\sigma \subsetneq \tau$. As regards condition (1) in the definition of coinductive strong subcontract relation, let $\mathbf{r}_1, \ldots, \mathbf{r}_n$ be the ready sets of σ. By contradiction, assume that there exists $\mathbf{r}'$ such that $\tau \Downarrow \mathbf{r}'$ and for every $1 \leq i \leq n$ there exists $\alpha_i \in \mathbf{r}_i$ such that $\alpha_i \notin \mathbf{r}'$. Let $\rho \stackrel{\text{def}}{=} \prod_{1 \leq i \leq n} \overline{\alpha_i}$.e. Then $\rho \dashv\vdash \sigma$ but $\rho \not\dashv\vdash \tau$, which is not possible. Hence condition (1) is satisfied. As regards condition (2) in the definition of coinductive strong subcontract relation, assume $\tau \xrightarrow{\alpha}$. By contradiction, assume $\sigma \not\xrightarrow{\alpha}$. Then $\mathrm{e} + \alpha \dashv\vdash \sigma$ but $\mathrm{e} + \alpha \not\dashv\vdash \tau$, which is not possible. Hence $\sigma \xrightarrow{\alpha}$. Now we have to prove that $\sigma(\alpha) \subsetneq \tau(\alpha)$. Let ρ' be such that $\rho' \dashv\vdash \sigma(\alpha)$. Then $\mathrm{e} + \alpha.\rho' \dashv\vdash \sigma$ hence $\mathrm{e} + \alpha.\rho' \dashv\vdash \tau$, thus $\rho' \dashv\vdash \tau(\alpha)$ by definition of strong compliance. Hence $\sigma(\alpha) \subsetneq \tau(\alpha)$ because ρ' is arbitrary.

Now we prove that $\subsetneq$ is indeed the largest coinductive subcontract relation, namely that every coinductive subcontract relation is included in $\subsetneq$. Let $\mathcal{S}$ be a coinductive strong subcontract relation and let $(\sigma, \tau) \in \mathcal{S}$. Let $\rho \dashv\vdash \sigma$, then there exists a strong compliance relation C such that $(\rho, \sigma) \in C$. To get $\rho \dashv\vdash \tau$ it is sufficient to prove that

$$C' \stackrel{\text{def}}{=} \{(\rho', \tau') \mid \exists \sigma', (\rho', \sigma') \in C \wedge (\sigma', \tau') \in \mathcal{S}\}$$

is a strong compliance relation, since $(\rho, \tau) \in C'$. Let $(\rho', \tau') \in C'$ and let σ' be the corresponding contract given by the definition of C'. As regards condition (1)

in Definition 2.6, let $\rho' \Downarrow \mathbf{r}$ and $\tau' \Downarrow s$. If $e \in \mathbf{r}$ there is nothing to prove. Assume $e \notin \mathbf{r}$. From $(\sigma', \tau') \in \mathcal{S}$ there exists $s' \subseteq s$ such that $\sigma' \Downarrow s'$. From $(\rho', \sigma') \in C$ we know $co(\mathbf{r}) \cap s' \neq \emptyset$, hence we conclude $co(\mathbf{r}) \cap s \neq \emptyset$. As regards condition (2) in Definition 2.6, assume $\rho' \xrightarrow{\overline{\alpha}}$ and $\tau' \xrightarrow{\alpha}$. From $(\sigma', \tau') \in \mathcal{S}$ we know that $\sigma' \xrightarrow{\alpha}$ and $(\sigma'(\alpha), \tau'(\alpha)) \in \mathcal{S}$. From $(\rho', \sigma') \in C$ we know that $(\rho'(\alpha), \sigma'(\alpha)) \in C$, hence we conclude $(\rho'(\alpha), \tau'(\alpha)) \in C'$ by definition of C'. □

It turns out that the relation $\subseteq$ is the *must testing preorder* as defined by [De Nicola and Hennessy 1984] (a proof can be found in [Laneve and Padovani 2007], where a different albeit equivalent notion of strong compliance is used). This relation is well studied and it enjoys interesting properties, in particular it is a precongruence with respect to prefixing, internal and external choices, and also $a \oplus b \subseteq a$, which is one of the desirable properties for $\dashv$, holds. However $\subseteq$ is stronger than $\dashv$ since, for example, $\overline{a}; \subseteq \overline{a} + \overline{b}$. Indeed $a.e + b \not\dashv \overline{a}$ but $a.e + b \not\dashv \overline{a} + \overline{b}$. In general, the must preorder allows neither width nor depth extensions of contracts.

In previous work [Carpineti et al. 2006] an attempt was made to directly relate two contracts σ and τ depending on their form, rather than on the sets of their clients. Let dual(σ) denote the dual contract of σ which, roughly, is obtained by replacing in σ every action by its coaction, $\mathbf{0}$ by e, every internal choice by an external one, and viceversa (the formal definition is slightly more involved and requires first to transform σ into the normal form of Definition 3.14 and then apply the transformation described above; see [Carpineti et al. 2006] for details). Intuitively dual(σ) denotes the contract of a "canonical" client complying with σ services. Then using this intuition one can informally define a new relation on service contracts as:

$$\sigma \dashv \tau \iff^{\text{def}} \text{dual}(\sigma) \not\dashv \tau \qquad (1)$$

In words, a contract σ is a subcontract of τ if and only if its canonical client complies with τ (see the proof of Theorem 3.4 for a formal definition of $\dashv$ and a more precise characterization of dual).

This relation is *nearly* what we are looking for. For instance now we have $a \oplus b.c \dashv a$ and $a \dashv a + b.d$, since $\text{dual}(a \oplus b.c) = \overline{a}.e + \overline{b}.\overline{c}.e \not\dashv a$ and $\text{dual}(a) = \overline{a}.e \not\dashv a + b.d$.

Unfortunately, $\dashv$ is not a preorder since transitivity does not hold: $\overline{a}.e + \overline{b}.\overline{c}.e; \not\dashv a + b.d$ implies that $a \oplus b.c; \dashv a + b.d$. The reason for such a failure is essentially due to the fact that in establishing $a \oplus b.c \dashv a$ and $a \dashv a + b.d$ we are restricting compliance to conversations in which no synchronization on the name b happens. While contracts account for non-determinism that is internal to each process—being it a client or a service—, they cannot handle the "system" non-determinism that springs from process synchronization. In the example above, the failure results from the interaction of two external choices, $\overline{a}.e + \overline{b}.\overline{c}.e$ and $a + b.d$, which yields non-determinism at system level and which does not prevent *a priori* a synchronization on the name b. By preventing the synchronization on the name b, the client $a.e + b.\overline{c}.e$ can terminate successfully.

In summary, the strong subcontract relation implements a safe substitutability relation for services that *are* compatible, but is excessively demanding because it takes into account every possible synchronization. Our theory of contracts will define a safe substitutability relation for services that *can be made* compatible.

3. THEORY OF CONTRACTS

At the end of the previous section we said that we wanted a subcontract relation $\sigma \leq \tau$ such that a service with contract τ *can be made* compatible with a service with contract σ. The keypoint of the discussion is the "can be made".

Of course we do not want to consider arbitrary transformations of the service, e.g. transformations that alter the semantics of the service. In fact, we cannot hope to affect in any way the internal non-determinism of a service as the service is typically considered as an unmodifiable black box. Instead we look for transformations that embed a τ service in a world of clients of σ servers so that such clients will perceive their interaction as being carried over a service with contract σ (or possibly a more deterministic one). Roughly speaking we want to filter out all behaviors of the τ contract that do not belong to the possible behaviors of σ world, and leave the others unchanged. This is, precisely, the characterization of an explicit coercion from τ to σ (recall that the subcontract relation is the inverse of a service subtyping relation; *cf.* Footnote 1 page 3): an embedding function that maps possible behaviors of τ into the same behaviors of σ (thus, it does not add new computation).

3.1 Weak subcontract relation

The idea is that $\sigma \leq \tau$ if there exists some (possibly empty) set of actions belonging to the world of τ that, if shielded, can make a τ service appear as a σ service. This is formalized by the following definition:

Definition 3.1 (weak subcontract). *W is a* weak subcontract relation *if $(\sigma, \tau) \in W$ implies that if $\tau \Downarrow \mathbf{r}$, then there exists $s_{\mathbf{r}} \subseteq \mathbf{r}$ such that (1) $\sigma \Downarrow s_{\mathbf{r}}$ and (2) for all $\alpha \in s_{\mathbf{r}}$ we have $(\sigma(\alpha), \tau(\alpha)) \in W$.*

We denote by $\leq$ the largest weak subcontract relation.

The basic intuition about the weak subcontract relation is that a client that interacts successfully with a service with contract σ must be able to complete whatever ready set is chosen from σ. If we want to replace the service with another one whose contract is τ, we require that whatever ready set $\mathbf{r}$ is chosen from τ there is a smaller one $s_{\mathbf{r}} \subseteq \mathbf{r}$ in σ such that all of the continuations with respect to the actions in $s_{\mathbf{r}}$ are in the weak subcontract relation. However, in order to avoid interferences we might need to filter out the actions in $\mathbf{r} \setminus s_{\mathbf{r}}$.

First of all notice that the weak subcontract relation includes the strong one (condition (1) is essentially the same and condition (2) is weaker), so that, for example, $a \oplus b.c \leq a$ holds. Additionally, we also have $a \leq a + b.d$ since a service with contract $a + b.d$ can be made to behave as a service with contract a by filtering out the b action. On the other hand, $a \not\leq a \oplus b.c$ since there is no way to make $a \oplus b.c$ behave as a by simply filtering out actions (filtering out the b action from $a \oplus b.c$ yields $a \oplus \mathbf{0}$, not a). Finally, we also have $a \oplus b.c \leq a + b.d$, again by filtering out the b action. In this case, the filtered service $(a + b.d)$ is not made equivalent to the smaller service $(a \oplus b.c)$ but rather to one of its more deterministic behaviors (a).

3.1.1 *Weak compliance.* In contrast with the "strong" case, for the weak subcontract relation it was more intuitive to provide its coinductive characterization first. We now face the problem of understanding which notion of compliance in-

duces the weak subcontract relation. As we will see, this is an essential intermediate step as it provides the necessary insight for devising the practical solution to the problems described in §2.4.

Definition 3.2 (weak compliance). *D is a* weak compliance relation *if* $(\rho, \sigma) \in D$ *implies that there exists a finite set of actions* $a \subseteq N \cup \overline{N}$ *such that:*

(*1*) $\rho \Downarrow \mathbf{r}$ *and* $\sigma \Downarrow s$ *implies* $e \in \mathbf{r}$ *or* $\mathrm{co}(\mathbf{r}) \cap a \cap s \neq \emptyset$, *and*

(*2*) $\alpha \in a$, $\rho \xrightarrow{\overline{\alpha}} \rho'$ *and* $\sigma \xrightarrow{\alpha} \sigma'$ *implies* $(\rho', \sigma') \in D$.

We denote by $\asymp$ *the largest weak compliance relation.*

The existence of the set a in the above definition is *independent* of the ready sets of the client and of the service. This reflects the fact that the internal non-determinism of the interacting parties cannot be affected.

The following theorem proves that $\asymp$ is the compliance relation inducing $\leq$.

Theorem 3.3. *$\sigma \leq \tau$ if and only if for all ρ, $\rho \asymp \sigma$ implies $\rho \asymp \tau$.*

Proof. ($\Rightarrow$) Let W be a weak subcontract relation such that $(\sigma, \tau) \in W$ and assume $\rho \asymp \sigma$. Let D be a weak compliance relation such that $(\rho, \sigma) \in D$. To get $\rho \asymp \tau$ it suffices to prove that

$$D' \stackrel{\text{def}}{=} \{(\rho', \tau') \mid \exists \sigma', (\rho', \sigma') \in D \wedge (\sigma', \tau') \in W\}$$

is a weak compliance relation since $(\rho, \tau) \in D'$. Let $(\rho', \tau') \in D'$, and let σ' be the corresponding contract given by the definition of D'. Let a' be the set of actions given by $(\rho', \sigma') \in D$. Let $s_1, \ldots, s_n$ be the ready sets of τ'. Because $(\sigma', \tau') \in W$, for each s_i there exists a ready set $s'_i \subseteq s_i$ of σ' which satisfies the conditions of Definition 3.1. Let $a \stackrel{\text{def}}{=} a' \cap \bigcup_{i=1}^{n} s'_i$. We now prove that this a satisfies the). As regards condition (1), assume $\rho' \Downarrow \mathbf{r}$ and $\tau' \Downarrow s$. Then $s = s_i$ for some i. If $e \in \mathbf{r}$ there is nothing to prove. Assume $e \notin \mathbf{r}$. Then from $(\rho', \sigma') \in D$ we know that $\mathrm{co}(\mathbf{r}) \cap a' \cap s'_i \neq \emptyset$. We have $a' \cap s'_i = a \cap s'_i \subseteq a \cap s_i$, hence we conclude $\mathrm{co}(\mathbf{r}) \cap a \cap s_i \neq \emptyset$. As regards condition (2), assume $\alpha \in a$ and $\rho' \xrightarrow{\overline{\alpha}}$ and $\tau' \xrightarrow{\alpha}$. Then $\sigma' \xrightarrow{\alpha}$, because α is in some s'_i; and α is also in a', thus $(\rho'(\alpha), \sigma'(\alpha)) \in D$ by definition of a'. From $\alpha \in s'_i$ we also have that $(\sigma'(\alpha), \tau'(\alpha)) \in W$. We conclude $(\rho'(\alpha), \tau'(\alpha)) \in D'$ by definition of D'.

($\Leftarrow$) We prove that

$$W \stackrel{\text{def}}{=} \{(\sigma, \tau) \mid \forall \rho, \rho \asymp \sigma \Rightarrow \rho \asymp \tau\}$$

is a weak subcontract relation. Let $(\sigma, \tau) \in W$. As regards condition (1) in Definition 3.1, let $\mathbf{r}_1, \ldots, \mathbf{r}_n$ be all the (distinct) ready sets of σ. By contradiction, suppose that there exists a ready set $\mathbf{r}'$ such that $\tau \Downarrow \mathbf{r}'$ and for every $1 \leq i \leq n$ we have $\mathbf{r}_i \not\subseteq \mathbf{r}'$, namely there exists $\alpha_i \in \mathbf{r}_i \setminus \mathbf{r}'$. Let $\rho \stackrel{\text{def}}{=} \bigsqcap_{1 \leq i \leq n} \overline{\alpha}_i$.e. By construction we have $\rho \asymp \sigma$ but $\rho \not\asymp \tau$, which is not possible. As regards condition (2) in Definition 3.1, let $\tau \Downarrow \mathbf{r}'$ and $k \in \{1, \ldots, n\}$ be such that $\mathbf{r}_k \subseteq \mathbf{r}'$ and $\mathbf{r}_k$ is *minimal* among the $\mathbf{r}_i$'s. We take $\mathbf{r}_k$ as the ready set $s_{\mathbf{r}}$ in the definition of weak subcontract relation. If $\mathbf{r}_k = \emptyset$, then condition (2) trivially holds. Assume $\mathbf{r}_k \neq \emptyset$.

For every $\alpha \in \mathbf{r}_k$, let ρ_α be a client contract such that $\rho_\alpha \dashv\vdash \sigma(\alpha)$. Notice that for every $i \in \{1, \ldots, n\} \setminus \{k\}$, we have $\mathbf{r}_i \setminus \mathbf{r}_k \neq \emptyset$ because the $\mathbf{r}_i$'s are all distinct and $\mathbf{r}_k$ is minimal. Let

$$\rho \stackrel{\text{def}}{=} \bigsqcap_{i \in \{1,\ldots,n\} \setminus \{k\}, \beta \in \mathbf{r}_i \setminus \mathbf{r}_k} \overline{\beta}.\mathbf{e} + \bigoplus_{\alpha \in \mathbf{r}_k} \overline{\alpha}.\rho_\alpha .$$

By construction $\rho \dashv\vdash \sigma$, hence $\rho \dashv\vdash \tau$ by definition of W. Furthermore, the set a in $\rho \dashv\vdash \sigma$ must be at least as large as $\mathbf{r}_k$ because, by construction of ρ, ρ cannot be (weakly) compliant with σ if any of the actions in $\mathbf{r}_k$ is filtered out. Thus, for every $\alpha \in \mathbf{r}_k$, from $\rho \dashv\vdash \sigma$ we derive $\rho_\alpha \dashv\vdash \sigma(\alpha)$, hence $\rho_\alpha \dashv\vdash \tau(\alpha)$. Because the ρ_α's are arbitrary, we conclude $(\sigma(\alpha), \tau(\alpha)) \in W$ by definition of W. □

3.1.2 *Comparison with other relations.* In §2.4 we said that the relation $\precsim$ defined by equation (1) was nearly what we sought for, but for the lack of transitivity it was not a preorder. The following theorem shows that $\precsim$ obviates this problem.

Theorem 3.4. *The subcontract relation $\precsim$ is the transitive closure of $\leqslant$.*

Proof. We did not define dual(σ) formally here, so we will give an equivalent definition of $\precsim$ not based on the notion of dual contract, which was also the definition used in [Carpineti et al. 2006], and just give the intuition of how we obtain it using dual(σ). The important property about dual(σ) is that its ready sets are defined as all the possible sets obtained by picking one action in each ready set of σ, and taking their co-actions. This can be seen by looking at the definition of observable ready sets and thinking that we just exchange internal and external choices. Now if we look at Definition 2.6 and assume $(\text{dual}(\sigma), \tau) \in C$ where C is a strong compliance relation, then the first condition says that any ready set of τ contains at least one action from each ready set of dual(σ), which is equivalent to the fact that it contains a ready set of σ. Translation of condition (2) is straightforward, so we get that $\precsim$ is the largest relation R such that $(\sigma, \tau) \in R$ implies:

(1) $\tau \Downarrow \mathbf{r}$ implies $\sigma \Downarrow \mathrm{s}$ for some $\mathrm{s} \subseteq \mathbf{r}$, and

(2) $\sigma \xrightarrow{\alpha}$ and $\tau \xrightarrow{\alpha}$ implies $(\sigma(\alpha), \tau(\alpha)) \in R$.

Now let us prove that $\precsim$ is the transitive closure of the relation thus defined. Note that the condition (1) is the same in both relations, and that condition (2) in Definition 3.1 is a weakened version of condition (1) for R, so obviously $\leqslant \subseteq \precsim$ and so does the transitive closure of $\leqslant$, $\precsim$ being itself transitive. So what we have to show is that two contracts related by $\precsim$ are also related by the transitive closure of $\leqslant$. Let W be a weak subcontract relation such that $(\sigma, \tau) \in W$. Let

$$R_1 \stackrel{\text{def}}{=} \{(\sigma, \bigoplus_{\tau \Downarrow \mathbf{r}} \bigsqcap_{\alpha \in \mathrm{S}_\mathbf{r}} \alpha.\sigma(\alpha)) \mid (\sigma, \tau) \in W\}$$
$$R_2 \stackrel{\text{def}}{=} \{(\bigoplus_{\tau \Downarrow \mathbf{r}} \bigsqcap_{\alpha \in \mathrm{S}_\mathbf{r}} \alpha.\sigma(\alpha), \tau) \mid (\sigma, \tau) \in W\}$$

where, for each ready set $\mathbf{r}$ of τ, we write $\mathrm{s}_\mathbf{r}$ for the ready set of σ such that $\mathrm{s}_\mathbf{r} \subseteq \mathbf{r}$ that satisfies condition (2) in Definition 3.1. It is trivial to verify that $R_1 \cup R_2 \subseteq \leqslant$, from which we conclude that W is included in the transitive closure of $\leqslant$. □

For what concerns the inclusion of the strong relation in the weak one note that if we compare Definition 3.1 with Definition 2.8, we see that they differ on the set of α's considered in condition (2). The latter requires that whatever interaction

may happen between a client and a server, the relation must be satisfied by the continuations. The former instead requires this to happen only for interactions on actions that are expected for the smaller contract. This means that with the weak subcontract relation all the actions that are not expected by the smaller contract *must not* take part in the client-server interaction. If we want to replace a server by a different server with a (weak) super-contract, then we must ensure that the client is shielded from these unexpected actions. The technical instrument to ensure it are the *filters* we define next.

3.2 Filters

A filter is the specification of a (possibly infinite) prefix-closed regular set of *traces*:

Definition 3.5 (filters). *A* filter *is a possibly infinite term coinductively generated by the following grammar.*

$$f ::= \mathbf{0} \mid \alpha.f \mid f \vee f \mid f \wedge f$$

and satisfying the following conditions:

(*1*) *filter terms are regular,*

(*2*) *on every infinite branch of a filter term there are infinitely many occurrences of the prefix constructor.*

The filter $\mathbf{0}$ is the one that allows no actions; the filter $\alpha.f$ allows those traces beginning with action α and followed by the traces allowed by f; the filter $f \vee g$ represents the *disjunction* of f and g and it allows those traces that are allowed either by f or by g; finally, the filter $f \wedge g$ represents the *conjunction* of f and g and it allows those traces that are allowed by both f and g. The conditions of regularity and contractivity are standard. The latter also provides a well-founded order for the induction used in the next definitions.

Much like contracts, filters too are equipped with the relations $\not\xrightarrow{\alpha}$ and $\xrightarrow{\alpha}$.

Definition 3.6 (filter transition). *Let $f \not\xrightarrow{\alpha}$ be the least relation such that:*

$$\mathbf{0} \not\xrightarrow{\alpha} \qquad \frac{\alpha \;;=\; \beta}{\beta.f \not\xrightarrow{\alpha}} \qquad \frac{f \not\xrightarrow{\alpha} \quad g \not\xrightarrow{\alpha}}{f \vee g \not\xrightarrow{\alpha}} \qquad \frac{f \not\xrightarrow{\alpha}}{f \wedge g \not\xrightarrow{\alpha}} \qquad \frac{g \not\xrightarrow{\alpha}}{f \wedge g \not\xrightarrow{\alpha}}$$

The transition relation *of filters, noted $\xrightarrow{\alpha}$, is the least relation satisfying the rules:*

$$\alpha.f \xrightarrow{\alpha} f \qquad \frac{f \xrightarrow{\alpha} f' \quad g \xrightarrow{\alpha} g'}{f \vee g \xrightarrow{\alpha} f' \vee g'} \qquad \frac{f \xrightarrow{\alpha} f' \quad g \not\xrightarrow{\alpha}}{f \vee g \xrightarrow{\alpha} f'} \qquad \frac{f \xrightarrow{\alpha} f' \quad g \xrightarrow{\alpha} g'}{f \wedge g \xrightarrow{\alpha} f' \wedge g'}$$

and closed under mirror cases for the disjunction. We write $f \xrightarrow{\alpha}$ if there exists f' such that $f \xrightarrow{\alpha} f'$.

This transition relation allows us to state more formally what we said above about sets of traces: the semantics of a filter is the prefix-closed regular language defined on the alphabet of actions by $[\![f]\!] \stackrel{\text{def}}{=} \{\varepsilon\} \cup \{\alpha\phi \mid f \xrightarrow{\alpha} f', \phi \in [\![f']\!]\}$. Then it can be easily checked that $[\![f \vee g]\!] = [\![f]\!] \cup [\![g]\!]$ and $[\![f \wedge g]\!] = [\![f]\!] \cap [\![g]\!]$ (notice that the intersection and the union of prefix-closed sets is again prefix-closed).

We consider two filters to be equal if they have the same semantics and adopt a notation similar to the one for contracts: we write $\bigvee_{i\in\{1,\ldots,n\}} f_i$ for $f_1 \vee f_2 \vee \cdots \vee f_n$ and $\bigwedge_{i\in\{1,\ldots,n\}} f_i$ for $f_1 \wedge f_2 \wedge \cdots \wedge f_n$. By convention we have $\bigvee_{i\in\emptyset} f_i = \mathbf{0}$. The application of a filter f to a contract σ, written $f(\sigma)$, produces another contract where only the allowed actions are visible:

Definition 3.7 (filter application). *The application of a filter f to a contract σ, written $f(\sigma)$, is inductively defined as follows:*

$$\begin{array}{rcll} f(\mathbf{0}) & = & \mathbf{0} & \\ f(\alpha.\sigma) & = & \mathbf{0} & \text{if } f \not\xrightarrow{\alpha} \\ f(\alpha.\sigma) & = & \alpha.f'(\sigma) & \text{if } f \xrightarrow{\alpha} f' \\ f(\sigma + \tau) & = & f(\sigma) + f(\tau) & \\ f(\sigma \oplus \tau) & = & f(\sigma) \oplus f(\tau) & \end{array}$$

Filter application is monotone with respect to the strong subcontract preorder. This property, which is fundamental in proving most of the results that follow, guarantees that equivalent contracts remain equivalent if filtered in the same way.

Proposition 3.8. *$\sigma \subsetneq \tau$ implies $f(\sigma) \subsetneq f(\tau)$.*

Proof. It is sufficient to show that

$$S \stackrel{\text{def}}{=} \{(f(\sigma), f(\tau)) \mid \sigma \subsetneq \tau\}$$

is a strong subcontract relation. Let $(f(\sigma), f(\tau)) \in S$. As regards condition (1) in the definition of strong subcontract relation, assume $f(\tau) \Downarrow s$. Then there exists s' such that $\tau \Downarrow s'$ and $s = f(s')$. From $\sigma \subsetneq \tau$ we derive that there exists $\mathbf{r}$ such that $\sigma \Downarrow \mathbf{r}$ and $\mathbf{r} \subseteq s'$. We observe $f(\mathbf{r}) \subseteq f(s') = s$ and we conclude by observing that $f(\sigma) \Downarrow f(\mathbf{r})$. As regards condition (2), assume $f(\tau) \xrightarrow{\alpha}$. Then $f \xrightarrow{\alpha} f'$ and $\tau \xrightarrow{\alpha}$. From the hypothesis $\sigma \subsetneq \tau$ we derive $\sigma \xrightarrow{\alpha}$ and $\sigma(\alpha) \subsetneq \tau(\alpha)$. We conclude $f(\sigma) \xrightarrow{\alpha}$ and $(f(\sigma)(\alpha), f(\tau)(\alpha)) \in S$ because $f(\sigma)(\alpha) = f'(\sigma(\alpha))$ and $f(\tau)(\alpha) = f'(\tau(\alpha))$. □

Filters allow us to express the weak subcontract relation in terms of the strong one:

Theorem 3.9. *$\sigma \leq \tau$ if and only if there exists a filter f such that $\sigma \subsetneq f(\tau)$.*

Proof. With an abuse of notation we write $f(\mathbf{r})$, the application of a filter f to a set of actions $\mathbf{r}$, for the set $\{\alpha \in \mathbf{r} \mid f \xrightarrow{\alpha}\}$.

(⇐) Let S be a coinductive strong subcontract relation. We show that

$$W \stackrel{\text{def}}{=} \{(\sigma, \tau) \mid \exists f, (\sigma, f(\tau)) \in S\}$$

is a weak subcontract relation. Let $(\sigma, \tau) \in W$ and let f be the corresponding filter. Regarding condition (1) in Definition 3.1, assume $\tau \Downarrow \mathbf{r}$. From $(\sigma, f(\tau)) \in S$ we know that there exists $s \subseteq f(\mathbf{r})$ such that $\sigma \Downarrow s$ and we conclude $s \subseteq f(\mathbf{r}) \subseteq \mathbf{r}$. Regarding condition (2) in Definition 3.1, take $\alpha \in s$. From $(\sigma, f(\tau)) \in S$ we know $(\sigma(\alpha), f_\alpha(\tau(\alpha))) \in S$ where $f \xrightarrow{\alpha} f_\alpha$. Hence we conclude $(\sigma(\alpha), \tau(\alpha)) \in W$.

(⇒) Let W be a weak subcontract relation. For every $(\sigma, \tau) \in W$, let

$$a(\sigma, \tau) \stackrel{\text{def}}{=} \bigcup_{\tau \Downarrow \mathbf{r}} s_{\mathbf{r}}$$

where $s_{\mathbf{r}} \subseteq \mathbf{r}$ is such that $\sigma \Downarrow s_{\mathbf{r}}$ and $s_{\mathbf{r}}$ satisfies condition (2) in Definition 3.1. Basically $a(\sigma, \tau)$ is the set of actions that need not be shielded for proving that $\sigma \not\asymp \tau$. Notice that $\alpha \in a(\sigma, \tau)$ implies $\sigma \xrightarrow{\alpha}$ and $\tau \xrightarrow{\alpha}$.

For every $(\sigma, \tau) \in W$, let

$$\boldsymbol{f}_{(\sigma,\tau)} \stackrel{\text{def}}{=} \bigvee_{\alpha \in a(\sigma,\tau)} \alpha.\boldsymbol{f}_{(\sigma(\alpha),\tau(\alpha))}\,.$$

Notice that, for every contract σ, the set $\{\sigma(\phi) \mid \sigma \xrightarrow{\phi}\}$ is finite because σ is regular. Hence, for every $(\sigma, \tau) \in W$, the set of pairs $\{(\sigma(\phi), \tau(\phi)) \mid \sigma \xrightarrow{\phi}, \tau \xrightarrow{\phi}\}$ is also finite, hence each $\boldsymbol{f}_{(\sigma,\tau)}$ is well defined, regular, and, by construction, also contractive. Now we prove that

$$\mathcal{S} \stackrel{\text{def}}{=} \{(\sigma, \boldsymbol{f}_{(\sigma,\tau)}(\tau)) \mid (\sigma, \tau) \in W\}$$

is a strong subcontract relation. Let $(\sigma, \boldsymbol{f}_{(\sigma,\tau)}(\tau)) \in \mathcal{S}$. As regards condition (1) in the definition of coinductive strong subcontract relation, assume $\tau \Downarrow \mathbf{r}$. By definition of $a(\sigma, \tau)$ there exists $s_{\mathbf{r}} \subseteq \mathbf{r}$ such that $\sigma \Downarrow s_{\mathbf{r}}$ and also $s_{\mathbf{r}} \subseteq a(\sigma, \tau)$, so we conclude $s_{\mathbf{r}} \subseteq \boldsymbol{f}_{(\sigma,\tau)}(\mathbf{r})$. As regards condition (2) in the definition of coinductive strong subcontract relation, assume $\boldsymbol{f}_{(\sigma,\tau)}(\tau) \xrightarrow{\alpha}$. Then $\tau \xrightarrow{\alpha}$ and there exists $s_{\mathbf{r}}$ such that $\sigma \Downarrow s_{\mathbf{r}}$ and $\alpha \in s_{\mathbf{r}}$, hence we obtain $\sigma \xrightarrow{\alpha}$ and $a(\sigma, \tau) \neq \emptyset$. From $(\sigma, \tau) \in W$ we derive $(\sigma(\alpha), \tau(\alpha)) \in W$ so we conclude $(\sigma(\alpha), \boldsymbol{f}_{(\sigma(\alpha),\tau(\alpha))}(\tau(\alpha))) \in \mathcal{S}$ by definition of $\mathcal{S}$. □

In terms of compliance this theorem yields the following corollary:

Corollary 3.10. *ρ -- σ if and only if there exists a filter $\boldsymbol{f}$ such that ρ -- $\boldsymbol{f}(\sigma)$*

Since -- ensures that a client will either continuously interact or successfully terminate with a strongly compliant service, this corollary tells us that filters are the operational device that ensures the same property in case of weak compliance. Properties of client/service interactions are formally stated in §4.

3.2.1 *Examples of filters.* Let us consider again our example of $\overline{a} \oplus \overline{b}.c$ and $\overline{a} + \overline{b}.d$. These contracts are not related by the strong subcontract relation, but any client complying with the first one has to be ready to read on a and then terminate. Then, we see that the second one *can be made* compliant with any such client, because it is ready to write on a: so we are sure that synchronization on a is possible, and that if it occurs the client will terminate. The point is then to ensure that this synchronization will indeed occur and that the channel b will not be selected instead, which would lead to a deadlock. This is done by applying to $\overline{a} + \overline{b}.d$ the filter $\boldsymbol{f} = \overline{a}$, which lets the sole action $\overline{a}$ pass. Formally, we have that $\boldsymbol{f}(\overline{a} + \overline{b}.d) = \overline{a}$, and $\overline{a} \oplus \overline{b}.c \subsetneq \overline{a}$ holds.

We have already hinted in the introduction that to prove an inclusion such as $a.b \not\asymp (a.(a+b)) + b.c$ filters must be able to selectively block along the computation, as b must be blocked only at the first step of the interaction and a only at the second step of the interaction. In this case the sought behavior is obtained by the single-threaded filter $\boldsymbol{f} = a.b$ which when applied to the contract on the right yields the one on the left. Such fine-grainedness of filters is useful also in practice. Consider again the last example of §2.2.2, where we extended the service by a "1-click ordering"

Table I. Deduction system for the weak subcontract relation.

(e1)	$\sigma + \sigma = \sigma$	(weak)	$\dfrac{f : \sigma \le \tau \quad g \wedge I(\tau) \quad f}{f \vee g : \sigma \le \tau}$
(e2)	$\sigma + \tau = \tau + \sigma$		
(e3)	$\sigma + (\sigma' + \sigma'') = (\sigma + \sigma') + \sigma''$	(trans)	$\dfrac{f : \sigma \le \sigma' \quad g : \sigma' \le \sigma''}{f \wedge g : \sigma \le \sigma''}$
(e4)	$\sigma + \mathbf{0} = \sigma$		
(i1)	$\sigma \oplus \sigma = \sigma$		
(i2)	$\sigma \oplus \tau = \tau \oplus \sigma$		
(i3)	$\sigma \oplus (\sigma' \oplus \sigma'') = (\sigma \oplus \sigma') \oplus \sigma''$	(Prefix)	$\dfrac{f : \sigma \le \tau}{\alpha.f : \alpha.\sigma \le \alpha.\tau}$
(d1)	$\sigma + (\sigma' \oplus \sigma'') = (\sigma + \sigma') \oplus (\sigma + \sigma'')$		
(d2)	$\sigma \oplus (\sigma' + \sigma'') = (\sigma \oplus \sigma') + (\sigma \oplus \sigma'')$	(IChoice)	$\dfrac{f : \sigma \le \sigma' \quad f : \tau \le \tau'}{f : \sigma \oplus \tau \le \sigma' \oplus \tau'}$
(d3)	$\alpha.\sigma + \alpha.\tau = \alpha.(\sigma \oplus \tau)$		
(d4)	$\alpha.\sigma \oplus \alpha.\tau = \alpha.(\sigma \oplus \tau)$		
(Must)	$I(\sigma) : \sigma \oplus \tau \le \sigma$	(EChoice)	$\dfrac{f : \sigma \le \sigma' \quad f : \tau \le \tau'}{f : \sigma + \tau \le \sigma' + \tau'}$
(Depth)	$\mathbf{0} : \mathbf{0} \le \sigma$		

capability. We said that backward compatibility can be obtained by filtering out the newly added Buy action. But if we slightly expand the resulting contract σ'

$$\ldots \overline{\text{Catalog}}.(\text{Logout}+\text{Buy}.\sigma_B+\text{AddToCart}.(\text{Logout}+\text{Buy}.(\ldots)))$$

we notice that there is also a Buy action after AddToCart. In order to make a service of contract σ' implement the contract σ defined in §2.2.2, one must block the Buy action offered right after the $\overline{\text{Catalog}}$ action, but allow the old Buy action in the continuation of AddToCart to pass through. This is performed by the filter obtained from σ by replacing $\vee$ for every sum (either internal or external) occurring in it.

3.3 Deduction system for the weak subcontract relation

Filters can also be used as proofs (in the sense of the Curry-Howard isomorphism) for the weak subcontract relation. More specifically, the idea is to devise a deduction system within which a derivable judgment of the form $f : \sigma \le \tau$ implies that $\sigma \not\simeq \tau$, and f is a filter that embeds services with contract τ into the world of σ-compliant clients.

The definition of such a deduction system requires a few auxiliary notions. First we have to define the "identity" filter, that is the one that proves isomorphic (with respect to an interpretation of filters as morphisms) contracts.

Definition 3.11. *The* identity filter *for a contract σ, denoted by $I(\sigma)$, is defined as*

$$I(\sigma) \stackrel{\text{def}}{=} \bigvee_{\sigma \xrightarrow{\alpha} \sigma} \alpha.I(\sigma')$$

It is easy to see that $I(\sigma)(\sigma) \simeq \sigma$.

Then, we need a way for comparing filters. Filters can be compared according to the actions that they let pass. In the deduction system the need for comparing filters arises naturally in the weakening rule, where we want to replace a filter with a "larger" one (a filter that allows more actions). This can be done safely only if the larger filter does not thwart the functionality of the original filter by re-introducing actions that must be kept hidden. The filter pre-order will also be fundamental in §3.4, in order to define the "best" filter that proves $\sigma \leq \tau$.

Definition 3.12 (filter order). *The ordering relation on filters is the largest relation such that $f \; g$ and $f \xrightarrow{\alpha} f'$ implies $g \xrightarrow{\alpha} g'$ and $f' \; g'$. We write $f = g$ for $f \; g$ and $g \; f$.*

In terms of filter semantics we have that $f \; g$ if and only if $[f] \subseteq [g]$. This set-theoretic interpretation gives us the relation between operators $\vee$ and $\wedge$ and filter ordering: the conjunction of two filters is their greatest lower bound, and their disjunction is their least upper bound.

Table I defines the deduction system for $\leq$. In the table we use a single axiom $\sigma = \tau$ as a shorthand for two axioms $I(\tau) : \sigma \leq \tau$ and $I(\sigma) : \tau \leq \sigma$. The equalities and rule (Must) are well known since they fully characterize the strong subcontract relation, which coincides with the must preorder [De Nicola and Hennessy 1984; Hennessy 1988]. Notice that in the rule (Must) no action needs to be actually filtered out and the filter $I(\sigma) \vee I(\tau)$ would work as well. In fact, this is the only axiom for safely enlarging a contract without the intervention of any filter (which is expected since this axiom characterizes strong compliance, where filters are not needed). Rule (Depth) formalizes *depth* extension of contracts, where a contract can be prolonged if no action is made visible from the continuation. Rule (Weak) shows how to safely enlarge a filter f to $f \vee g$: the premise $g \wedge I(\tau) \; f$ states that g may allow actions not allowed by f, provided that such actions are not those that have been hidden for the purposes of proving $f : \sigma \leq \tau$. Rule (Trans) is standard and the resulting filter is the composition filter. Three forms of (limited) pre-congruence follow. Rule (Prefix) is standard and poses no constraints. Rules (IChoice) and (EChoice) state the limited precongruence property for internal and external choices, respectively. The fundamental constraint is that two contracts combined by means of $\oplus$ or $+$ can be enlarged, provided that they can be filtered in the same way. This requirement has an intuitive explanation: the filter that mediates the interaction of a client with a service is unaware of the internal choices that have been taken by the parties at a branching point. So, it must be possible to use *the same* filter that works equally well in all branches in order for the branches to be enlarged.

3.3.1 *Properties.* First of all notice that the deductions of the system we devised in the previous section may be infinite. However valid deductions are regular and contractive. This is a direct consequence of the regularity and contractivity of both contracts and filters. This is easily seen by observing that every deduction rule on the right hand side of Table I deconstructs in its premises either the filter or the contracts that occur in its consequence. This implies that infinite valid derivations are regular and that on every infinite branch of the derivation there are infinitely many applications of the rule (Prefix).

The deduction system is sound and complete with respect to $\leq$ *and* the set of filters, in the sense that it proves all and only the pairs of contracts that are related according to Definition 3.1, and for any such pair it deduces all and only the filters that validate the pair according to Theorem 3.9.

Theorem 3.13 (soundness). *If* $f : \sigma \leq \tau$, *then* $\sigma \subsetneq f(\tau)$.

Proof. Let S be the least relation such that if $f : \sigma \leq \tau$ is derivable, then $(\sigma, f(\tau)) \in S$. It is sufficient to prove that S is a coinductive strong subcontract relation. Suppose $f : \sigma \leq \tau$ is derivable, then $(\sigma, f(\tau)) \in S$. We have to prove that $f(\tau) \Downarrow \mathbf{r}$ implies $\sigma \Downarrow \mathbf{r}'$ and $\mathbf{r}' \subseteq \mathbf{r}$ and that $f(\tau) \xrightarrow{\alpha}$ implies $\sigma \xrightarrow{\alpha}$ and $(\sigma(\alpha), f(\alpha)(\tau(\alpha))) \in S$. We do so by induction on the maximum depth of an axiom or of an unnested instance of rule (Prefix) in the derivation tree of $f : \sigma \leq \tau$ and by cases on the last rule applied. Such depth is always finite because contracts are contractive (hence, any infinite branch of the derivation tree must contain infinitely many instances of rule (Prefix)). In the following we only show the nontrivial cases.

Assume the last rule was (Prefix). Then $\sigma \equiv \alpha.\sigma'$, $f \equiv \alpha.f'$, $\tau \equiv \alpha.\tau'$, and $f' : \sigma' \leq \tau'$ is derivable (we use $\equiv$ to denote syntactic equality). Suppose $f(\tau) \Downarrow \mathbf{r}$. Then $\mathbf{r} = \{\alpha\}$ and we notice that $\sigma \Downarrow \{\alpha\}$. We also notice that $\tau \xrightarrow{\alpha}$ and $\sigma \xrightarrow{\alpha}$ and that this is the only possible transition for σ and τ. Furthermore, $\sigma(\alpha) \equiv \sigma'$, $f(\alpha) \equiv f'$, and $\tau(\alpha) \equiv \tau'$, and we conclude because $f' : \sigma' \leq \tau'$ is derivable by hypothesis, hence $(\sigma(\alpha), f(\alpha)(\tau(\alpha))) \in S$ by definition of S.

Assume the last rule was (Must). Then $\sigma \equiv \sigma' \oplus \tau$ and $f \equiv I(\tau)$. Suppose $f(\tau) \Downarrow \mathbf{r}$. Then $\tau \Downarrow \mathbf{r}$ and $\sigma \Downarrow \mathbf{r}$. Suppose $f(\tau) \xrightarrow{\alpha}$. We have two subcases: if $\sigma' \xrightarrow{\alpha}$, then $\sigma(\alpha) \equiv \sigma'(\alpha) \oplus \tau(\alpha)$ and we conclude $f(\alpha) : \sigma'(\alpha) \oplus \tau(\alpha) \leq \tau(\alpha)$ by (Must). If $\sigma' \not\xrightarrow{\alpha}$, then $\sigma(\alpha) \equiv \tau(\alpha)$, hence we conclude by reflexivity of $\leq$ (indeed $\sigma = \sigma \oplus \sigma$ and $I(\sigma) : \sigma \oplus \sigma \leq \sigma$).

Assume the last rule was (Depth). Then $\sigma \equiv \mathbf{0}$ and $f \equiv \mathbf{0}$. The condition on ready sets of $f(\tau)$ trivially holds because $\sigma \Downarrow \emptyset$. Furthermore $f(\tau) \not\xrightarrow{\alpha}$ for every α.

Assume the last rule was (Weak). Then $f \equiv f' \vee g$, $f' : \sigma \leq \tau$, and $g \wedge I(\tau) \not\simeq f'$. Suppose $f(\tau) \Downarrow \mathbf{r}$. Since by definition f is less restrictive than f', there is a $\mathbf{r}' \subseteq \mathbf{r}$ such that $f'(\tau) \Downarrow \mathbf{r}'$. By induction hypothesis, σ has a ready set $\mathbf{r}''$ such that $\mathbf{r}'' \subseteq \mathbf{r}'$, hence we conclude $\mathbf{r}'' \subseteq \mathbf{r}$. Suppose $f(\tau) \xrightarrow{\alpha}$. We have two subcases. If $g \xrightarrow{\alpha}$, then $f(\alpha) \equiv f'(\alpha) \vee g(\alpha)$ and $g(\alpha) \wedge I(\tau(\alpha)) \not\simeq f'(\alpha)$. By induction hypothesis $\sigma \xrightarrow{\alpha}$ and $f'(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$ is derivable, hence we derive $f(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$ by (Weak), so we conclude $(\sigma(\alpha), f(\alpha)(\tau(\alpha))) \in S$ by definition of S. If $g \not\xrightarrow{\alpha}$, then $f(\alpha) \equiv f'(\alpha)$. By induction hypothesis $\sigma \xrightarrow{\alpha}$ and $f'(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$, hence $(\sigma(\alpha), f(\alpha)(\tau(\alpha))) \in S$ by definition of S.

Assume the last rule was (Trans). Then $f \equiv f' \wedge g$, $f' : \sigma \leq \sigma'$, $g : \sigma' \leq \tau$. Suppose $\tau \Downarrow \mathbf{r}$. By induction hypothesis σ' has a ready set $\mathbf{r}'$ such that $\mathbf{r}' \subseteq g(\mathbf{r})$. By induction hypothesis σ has a ready set $\mathbf{r}''$ such that $\mathbf{r}'' \subseteq f'(\mathbf{r}') \subseteq f'(g(\mathbf{r})) = f(\mathbf{r})$. Suppose $f(\tau) \xrightarrow{\alpha}$. Then $g(\tau) \xrightarrow{\alpha}$. By induction hypothesis $\sigma' \xrightarrow{\alpha}$ and $g(\alpha) : \sigma'(\alpha) \leq \tau(\alpha)$ is derivable. From $f(\tau) \xrightarrow{\alpha}$ we also derive $f' \xrightarrow{\alpha}$, hence $f'(\sigma') \xrightarrow{\alpha}$. Again by induction hypothesis, $\sigma \xrightarrow{\alpha}$ and $f'(\alpha) : \sigma(\alpha) \leq \sigma'(\alpha)$ is derivable. By (Trans) we conclude that $f(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$ is derivable.

Assume the last rule was (IChoice). Then $\sigma \equiv \sigma' \oplus \tau'$, $\tau \equiv \sigma'' \oplus \tau''$, $f : \sigma' \leq \sigma''$,

and $\mathcal{F} : \tau' \leq \tau''$. Suppose $\mathcal{F}(\tau) \Downarrow \mathbf{r}$ and assume, without loss of generality, that $\mathcal{F}(\tau'') \Downarrow \mathbf{r}$. By induction hypothesis we obtain $\mathbf{r}'$ such that $\tau' \Downarrow \mathbf{r}'$ and $\mathbf{r}' \subseteq \mathbf{r}$. We conclude by observing that $\sigma \Downarrow \mathbf{r}'$. Suppose $\mathcal{F}(\tau) \xrightarrow{\alpha}$. We have three subcases, depending on which contracts between σ'' and τ'' admit α-successors. Assume $\sigma'' \xrightarrow{\alpha}$ and $\tau'' \xrightarrow{\alpha}$. By induction hypothesis $\sigma' \xrightarrow{\alpha}$ and $\tau' \xrightarrow{\alpha}$ and $\mathcal{F}(\alpha) : \sigma'(\alpha) \leq \sigma''(\alpha)$ is derivable and $\mathcal{F}(\alpha) : \tau'(\alpha) \leq \tau''(\alpha)$ is derivable. Then we conclude $\mathcal{F}(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$ is also derivable because $\sigma(\alpha) \equiv \sigma'(\alpha) \oplus \tau'(\alpha)$ and $\tau(\alpha) \equiv \sigma''(\alpha) \oplus \tau''(\alpha)$. On the other hand, suppose $\sigma'' \xrightarrow{\alpha}$ but $\tau'' \not\xrightarrow{\alpha}$. By induction hypothesis $\sigma' \xrightarrow{\alpha}$ and $\mathcal{F}(\alpha) : \sigma'(\alpha) \leq \sigma''(\alpha)$ is derivable. We distinguish two further subcases. Either (*i*) $\tau' \xrightarrow{\alpha}$ or (*ii*) $\tau' \not\xrightarrow{\alpha}$. In subcase (*i*) we have $\sigma(\alpha) \equiv \sigma'(\alpha) \oplus \tau'(\alpha)$. By (Must) we derive $\mathcal{I}(\sigma'(\alpha)) : \sigma(\alpha) \leq \sigma'(\alpha)$, from $\mathcal{F}(\alpha) \wedge \mathcal{I}(\sigma'(\alpha))$ $\mathcal{I}(\sigma'(\alpha))$ and (weak) we obtain $\mathcal{F}(\alpha) : \sigma(\alpha) \leq \sigma'(\alpha)$ and now we conclude $\mathcal{F}(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$ by (trans) and noticing that $\tau(\alpha) \equiv \sigma''(\alpha)$. In subcase (*ii*) we have $\sigma(\alpha) \equiv \sigma'(\alpha)$ and now $\mathcal{F}(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$ is derivable by hypothesis.

Assume the last rule was (EChoice). Then we can proceed as for the previous case, the only thing that changes being the reasoning on ready sets. The details are left to the reader. □

While the soundness of the deduction system can be easily established, its completeness is less immediate, but the proof of this fact follows a standard pattern: completeness is proved for a restricted class of contracts which are said to be in some normal form and then it is shown that it is always possible to rewrite an arbitrary contract to an equivalent one which is in normal form by using the axioms.

As regards the actual definition of the normal form, we notice that it is always possible to add new ready sets to a given contract σ without altering its semantics (according to $\simeq$), so long as $\mathcal{I}(\sigma)$ does not change and the new ready sets contain older ones: for example, $\sigma \oplus \tau \simeq \sigma \oplus \tau \oplus (\sigma + \tau)$. If we saturate the set of ready sets of a contract by adding to it every possible ready set meeting the conditions above, we can build a unique (up to commutativity and associativity) normal form for each equivalence class. This normal form is defined as follows:

Definition 3.14 (normal form [Hennessy 1988]). *For any contract σ, we define its saturated set of ready sets:*

$$R(\sigma) \stackrel{\text{def}}{=} \{\mathbf{r} \subseteq \text{init}(\sigma) \mid \exists s, \sigma \Downarrow s \wedge s \subseteq \mathbf{r}\}$$

The normal form of σ is then defined up to associativity and commutativity of the choices by the following recursive expression:

$$\text{nf}(\sigma) \stackrel{\text{def}}{=} \bigoplus_{\mathbf{r} \in R(\sigma)} \sum_{\alpha \in \mathbf{r}} \alpha.\text{nf}(\sigma(\alpha))$$

the empty external choice being defined as $\mathbf{0}$ *(it is not necessary to define the empty internal choice, because any contract has at least one ready set). Notice that* $\text{nf}(\sigma)$ *is well defined because σ is regular, hence $\{\sigma(\phi) \mid \sigma \xrightarrow{\phi}\}$ is finite.*

The normal form enjoys the following properties: (1) In a given mix of internal and external choices (either at top-level or under a given sequence of prefixes), a prefix α is always followed by the exact same continuation. (2) If σ and τ are two

Table II. Derived rules.

(s1)	$\sigma \oplus \tau = \sigma \oplus \tau \oplus (\sigma + \tau)$	(C-Prefix)	$\dfrac{\sigma = \sigma}{\alpha.\sigma = \alpha.\sigma}$
(s2)	$\sigma \oplus (\sigma + \tau + \rho) = \sigma \oplus (\sigma + \tau) \oplus (\sigma + \tau + \rho)$		
(co)	$(\alpha.\sigma + \tau) \oplus (\alpha.\sigma + \tau) = (\alpha.(\sigma \oplus \sigma) + \tau) \oplus (\alpha.(\sigma \oplus \sigma) + \tau)$	(C-EChoice)	$\dfrac{\sigma = \sigma \quad \tau = \tau}{\sigma + \tau = \sigma + \tau}$
(Width)	$\dfrac{I(\sigma) \wedge I(\tau) \quad \mathbf{0}}{I(\sigma) : \sigma \leq \sigma + \tau}$	(C-IChoice)	$\dfrac{\sigma = \sigma \quad \tau = \tau}{\sigma \oplus \tau = \sigma \oplus \tau}$

normal form contracts such that $\sigma \subsetneq \tau$, condition (1) of the strong subcontract relation holds if and only if every ready set of τ is also a ready set of σ. These two properties lead to the fact that two equivalent normal forms are syntactically equal up to commutativity and associativity of the choice operators.

To prove that every contract can be rewritten to an equivalent one in normal form it is useful to derive a handful of auxiliary axioms and rules (Table II) that will be fundamental in the following. Axioms (s1) and (s2) will be used for saturating ready sets as required by the definition of normal form. Axiom (co) shows that it is possible to rewrite a contract so that all the continuations under the same prefix α are equal. Rules (C-Prefix), (C-IChoice), and (C-EChoice) are strengthened versions of rules (Prefix), (IChoice), and (EChoice) showing the congruence properties of $=$ with respect to the prefix and the two choices. Such rules will allow us to replace equivalent contracts in arbitrary contexts. Finally, rule (Width) states that a service can be extended with additional capabilities, provided that such capabilities are disjoint from those that were available before the extension.

Lemma 3.15. *The axioms and rules in Table II are derivable from those in Table I.*

Proof. In the rewritings that follow we indicate only the most relevant laws that are applied. As regards (s1):

$$\begin{aligned} \sigma \oplus \tau &= (\sigma \oplus \tau) + (\sigma \oplus \tau) && (1)\\ &= \sigma \oplus \tau \oplus (\sigma + \tau) && (2) \end{aligned}$$

where (1) is justified by (e1) and (2) is justified by (d1).

As regards (s2):

$$\begin{aligned} \sigma \oplus (\sigma + \tau + \rho) &= \sigma + (\sigma \oplus \tau) + (\sigma \oplus \rho) && (1)\\ &= \sigma + (\sigma \oplus (\sigma + \tau) \oplus (\sigma + \rho) \oplus (\tau + \rho)) && (2)\\ &= \sigma \oplus (\sigma + \tau) \oplus (\sigma + \rho) \oplus (\sigma + \tau + \rho) && (3)\\ &= \sigma \oplus (\sigma + \tau) \oplus (\sigma + \tau) \oplus (\sigma + \rho) \oplus (\sigma + \tau + \rho) && (4)\\ &= \sigma \oplus (\sigma + \tau) \oplus (\sigma + \tau + \rho) && (5) \end{aligned}$$

where (1) is justified by (d2), (2) is justified by (d1), (3) is justified by (d2), (4) is justified by (i1) and finally (5) is justified by rewriting the subterm of step (3) with the original one.

As regards (co):

$$
\begin{aligned}
&(\alpha.\sigma + \tau) \oplus (\alpha.\sigma' + \tau') \\
&\quad = (\alpha.\sigma + \tau) \oplus (\alpha.\sigma' + \tau') \oplus (\alpha.\sigma + \alpha.\sigma' + \tau + \tau') && (1)\\
&\quad = (\alpha.\sigma + \tau) \oplus (\alpha.\sigma' + \tau') \oplus (\alpha.\sigma + \alpha.\sigma' + \tau + \tau') \\
&\qquad \oplus (\alpha.\sigma + \alpha.\sigma' + \tau) \oplus (\alpha.\sigma + \alpha.\sigma' + \tau') && (2)\\
&\quad = (\alpha.\sigma + \tau) \oplus (\alpha.\sigma' + \tau') \oplus (\alpha.\sigma + \alpha.\sigma' + \tau + \tau') \\
&\qquad \oplus (\alpha.(\sigma \oplus \sigma') + \tau) \oplus (\alpha.(\sigma \oplus \sigma') + \tau') && (3)\\
&\quad = (\alpha.\sigma + \tau) \oplus (\alpha.\sigma' + \tau') \oplus (\alpha.(\sigma \oplus \sigma') + \tau) \oplus (\alpha.(\sigma \oplus \sigma') + \tau') && (4)\\
&\quad = ((\alpha.\sigma \oplus \alpha.(\sigma \oplus \sigma')) + \tau) \oplus ((\alpha.\sigma' \oplus \alpha.(\sigma \oplus \sigma')) + \tau') && (5)\\
&\quad = (\alpha.(\sigma \oplus \sigma') + \tau) \oplus (\alpha.(\sigma \oplus \sigma') + \tau') && (6)
\end{aligned}
$$

where (1) is justified by (s1), (2) is justified by (s2), (3) is justified by (d3), (4) is justified by (s1), (5) is justified by (d1), and (6) is justified by (d4) and (i1).

Proving (C-Prefix) is trivial. As regards (C-EChoice), observe that from $I(\sigma') : \sigma \leq \sigma'$ and $I(\tau') \wedge I(\sigma') \vdash I(\sigma')$ we derive $I(\sigma') \vee I(\tau') : \sigma \leq \sigma'$ by an application of (Weak). Similarly we can derive $I(\sigma') \vee I(\tau') : \tau \leq \tau'$, hence we can apply (EChoice) and derive $I(\sigma') \vee I(\tau') : \sigma + \tau \leq \sigma' + \tau'$. By a similar argument we can also derive $I(\sigma) \vee I(\tau) : \sigma' + \tau' \leq \sigma + \tau$, hence $\sigma + \tau = \sigma' + \tau'$. Rule (C-IChoice) is analogous.

As regards (Width), from the axiom $\mathbf{0} : \mathbf{0} \leq \tau$ and the hypothesis $I(\sigma) \wedge I(\tau) \vdash \mathbf{0}$ we derive $I(\sigma) : \mathbf{0} \leq \tau$. From $I(\sigma) : \sigma \leq \sigma$ and applying (EChoice) we conclude $I(\sigma) : \sigma + \mathbf{0} \leq \sigma + \tau$, hence $I(\sigma) : \sigma \leq \sigma + \tau$. □

We are now ready to prove that every contract can be rewritten into its own normal form.

Lemma 3.16 (normal form). *The judgment* $\sigma = \mathrm{nf}(\sigma)$ *is derivable.*

Proof. We define the *head normal form* of σ as $\mathrm{hnf}(\sigma) \stackrel{\text{def}}{=} \bigoplus_{\mathbf{r} \in R(\sigma)} \sum_{\alpha \in \mathbf{r}} \alpha.\sigma(\alpha)$. It is sufficient to prove that $\sigma = \mathrm{hnf}(\sigma)$ is derivable because then what remains to prove is $\sigma(\alpha) = \mathrm{hnf}(\sigma(\alpha))$, but since σ is regular the number of these proofs is the same as the cardinality of $\{\sigma(\phi) \mid \sigma \xrightarrow{\phi}\}$, which is finite, hence the (possibly infinite) proof of $\sigma = \mathrm{nf}(\sigma)$ is regular.

We prove $\sigma = \mathrm{hnf}(\sigma)$ by induction on the maximum depth of a topmost prefix in σ and by cases on the structure of σ. If $\sigma \equiv \mathbf{0}$, then σ is already in head normal form.

If $\sigma \equiv \alpha.\sigma'$, then σ is already in head normal form because $\sigma(\alpha)$ is σ'.

If $\sigma \equiv \sigma_1 + \sigma_2$, then

$$
\begin{aligned}
\sigma &= \Big(\bigoplus_{\mathbf{r}_1 \in R(\sigma_1)} \sum_{\alpha \in \mathbf{r}_1} \alpha.\sigma_1(\alpha)\Big) + \Big(\bigoplus_{\mathbf{r}_2 \in R(\sigma_2)} \sum_{\beta \in \mathbf{r}_2} \beta.\sigma_2(\beta)\Big) && (1)\\
&= \bigoplus_{\mathbf{r}_1 \in R(\sigma_1), \mathbf{r}_2 \in R(\sigma_2)} \Big(\sum_{\alpha \in \mathbf{r}_1} \alpha.\sigma_1(\alpha) + \sum_{\beta \in \mathbf{r}_2} \beta.\sigma_2(\beta)\Big) && (2)\\
&= \bigoplus_{\mathbf{r}_1 \in R(\sigma_1), \mathbf{r}_2 \in R(\sigma_2)} \sum_{\alpha \in \mathbf{r}_1 \cup \mathbf{r}_2} \alpha.\sigma(\alpha) && (3)\\
&= \bigoplus_{\mathbf{r} \in R(\sigma)} \sum_{\alpha \in \mathbf{r}} \alpha.\sigma(\alpha) && (4)
\end{aligned}
$$

where (1) is justified by the induction hypothesis and congruence rules, (2) is justified by the repeated use of (d1), (3) is justified by (co), and (4) follows from $R(\sigma) = \{\mathbf{r}_1 \cup \mathbf{r}_2 \mid \mathbf{r}_1 \in R(\sigma_1), \mathbf{r}_2 \in R(\sigma_2)\}$. Indeed, if $\mathbf{r} \in R(\sigma)$, then there exist $\mathbf{r}_1'$ and $\mathbf{r}_2'$ such that $\sigma_1 \Downarrow \mathbf{r}_1'$ and $\sigma_2 \Downarrow \mathbf{r}_2'$ and $\mathbf{r}_1' \cup \mathbf{r}_2' \subseteq \mathbf{r}$. Now $\mathbf{r}_1' \subseteq \mathbf{r} \cap \mathrm{init}(\sigma_1) \subseteq \mathrm{init}(\sigma_1)$ and $\mathbf{r}_2' \subseteq \mathbf{r} \cap \mathrm{init}(\sigma_2) \subseteq \mathrm{init}(\sigma_2)$, hence

$\mathbf{r} \cap \mathrm{init}(\sigma_1) \in R(\sigma_1)$ and $\mathbf{r} \cap \mathrm{init}(\sigma_2) \in R(\sigma_2)$. We conclude by observing that $(\mathbf{r} \cap \mathrm{init}(\sigma_1)) \cup (\mathbf{r} \cap \mathrm{init}(\sigma_2)) = \mathbf{r}$ because $\mathbf{r} \subseteq \mathrm{init}(\sigma_1) \cup \mathrm{init}(\sigma_2)$. On the other hand, let $\mathbf{r}_1 \in R(\sigma_1)$ and $\mathbf{r}_2 \in R(\sigma_2)$. Then there exist ready sets $\mathbf{r}'_1$ and $\mathbf{r}'_2$ of respectively σ_1 and σ_2 such that $\mathbf{r}'_1 \subseteq \mathbf{r}_1 \subseteq \mathrm{init}(\sigma_1)$ and $\mathbf{r}'_2 \subseteq \mathbf{r}_2 \subseteq \mathrm{init}(\sigma_2)$. Hence $\mathbf{r}'_1 \cup \mathbf{r}'_2 \subseteq \mathbf{r}_1 \cup \mathbf{r}_2 \subseteq \mathrm{init}(\sigma_1) \cup \mathrm{init}(\sigma_2)$ and we conclude $\mathbf{r}_1 \cup \mathbf{r}_2 \in R(\sigma)$ by observing $\sigma \xrightarrow{\mathbf{r}'_1} \xrightarrow{\mathbf{r}'_2}$ and $\mathrm{init}(\sigma) = \mathrm{init}(\sigma_1) \cup \mathrm{init}(\sigma_2)$.

Finally, if $\sigma \equiv \sigma_1 \oplus \sigma_2$, then

$$\begin{aligned} \sigma &= \Big(\bigoplus_{\mathbf{r}_1 \in R(\sigma_1)} \sum_{\alpha \in \mathbf{r}_1} \alpha.\sigma_1(\alpha)\Big) \oplus \Big(\bigoplus_{\mathbf{r}_2 \in R(\sigma_2)} \sum_{\beta \in \mathbf{r}_2} \beta.\sigma_2(\beta)\Big) && (1)\\ &= \Big(\bigoplus_{\mathbf{r}_1 \in R(\sigma)} \sum_{\alpha \in \mathbf{r}_1} \alpha.\sigma(\alpha)\Big) \oplus \Big(\bigoplus_{\mathbf{r}_2 \in R(\sigma)} \sum_{\beta \in \mathbf{r}_2} \beta.\sigma(\beta)\Big) && (2)\\ &= \bigoplus_{\mathbf{r} \in R(\sigma)} \sum_{\alpha \in \mathbf{r}} \alpha.\sigma(\alpha) && (3) \end{aligned}$$

where (1) is justified by the induction hypothesis and congruence rules, (2) is justified by (co), and (3) is justified by the repeated use of (s1) and (s2). □

We now possess all the technical tools to prove that the deduction system shown in Table I is complete for $\preceq$ and the sets of filters that prove it.

Theorem 3.17 (completeness). *If $\sigma \subsetneq \boldsymbol{f}(\tau)$, then $\boldsymbol{f} : \sigma \leq \tau$.*

Proof. By Lemma 3.16 we can assume that σ and τ are in normal form. Additionally, for the sake of simplicity we identify $\sigma(\alpha)$, $\tau(\alpha)$, and $\boldsymbol{f}(\tau)$ with their corresponding normal forms (indeed $\mathrm{nf}(\sigma(\alpha))$, $\mathrm{nf}(\tau(\alpha))$, and $\mathrm{nf}(\boldsymbol{f}(\tau(\alpha)))$ can be obtained from $\sigma(\alpha)$, $\tau(\alpha)$, and $\boldsymbol{f}(\tau)$ by repeated use of (i1)).

Let $P(\boldsymbol{f}, \sigma, \tau)$ stand for the proof tree whose conclusion is $\boldsymbol{f} : \sigma \leq \tau$. Below we will show that $P(\boldsymbol{f}, \sigma, \tau)$ can be built provided that proof trees $P(\boldsymbol{f}(\alpha), \sigma(\alpha), \tau(\alpha))$ are available for all α such that $\sigma \xrightarrow{\alpha}$ and $\boldsymbol{f}(\tau) \xrightarrow{\alpha}$. However, the set $\{(\boldsymbol{f}(\phi), \sigma(\phi), \tau(\phi)) \mid \boldsymbol{f} \xrightarrow{\phi}, \sigma \xrightarrow{\phi}, \tau \xrightarrow{\phi}\}$ is finite because $\boldsymbol{f}$, σ, and τ are regular. Hence, we overall need to show how to build a finite number of proofs $P(\boldsymbol{f}(\phi), \sigma(\phi), \tau(\phi))$ and so the possibly infinite proof of $P(\boldsymbol{f}, \sigma, \tau)$ is also regular.

If $\tau \equiv \mathbf{0}$, then σ must have an empty ready set hence by (Must) we have $\mathbf{0} : \sigma \leq \mathbf{0}$ and we conclude $\boldsymbol{f} : \sigma \leq \tau$ by (Weak) because $\boldsymbol{f} \wedge \boldsymbol{I}(\mathbf{0}) \simeq \mathbf{0}$.

For the remaining cases, assume

$$\sigma \equiv \bigoplus_{\mathbf{r} \in R(\sigma)} \sum_{\alpha \in \mathbf{r}} \alpha.\sigma(\alpha) \qquad \text{and} \qquad \tau \equiv \bigoplus_{\mathbf{s} \in R(\tau)} \sum_{\alpha \in \mathbf{s}} \alpha.\tau(\alpha)$$

and assume $\boldsymbol{f}(\tau) \xrightarrow{\alpha}$. From $\sigma \subsetneq \boldsymbol{f}(\tau)$ we have $\sigma \xrightarrow{\alpha}$ and from the proof $P(\boldsymbol{f}(\alpha), \sigma(\alpha), \tau(\alpha))$ we derive

$$\boldsymbol{f}(\alpha) : \sigma(\alpha) \leq \tau(\alpha)$$

then, by (Prefix),

$$\alpha.\boldsymbol{f}(\alpha) : \alpha.\sigma(\alpha) \leq \alpha.\tau(\alpha)\,.$$

Now assume $\tau \Downarrow \mathbf{r}$. From $\sigma \subsetneq \boldsymbol{f}(\tau)$ and the fact that σ and τ are in head normal form we have $\sigma \Downarrow \boldsymbol{f}(\mathbf{r})$. Let $\boldsymbol{f}_{\mathbf{r}} \stackrel{\text{def}}{=} \bigvee_{\alpha \in \boldsymbol{f}(\mathbf{r})} \alpha.\boldsymbol{f}(\alpha)$ and notice that $\boldsymbol{f}_{\mathbf{r}} \wedge \alpha.\boldsymbol{I}(\tau(\alpha)) \simeq \alpha.\boldsymbol{f}(\alpha)$. Hence, by (Weak),

$$\boldsymbol{f}_{\mathbf{r}} : \alpha.\sigma(\alpha) \leq \alpha.\tau(\alpha)$$

and, by (EChoice),

$$\boldsymbol{f}_{\mathbf{r}} : \bigwedge_{\alpha \in \boldsymbol{f}(\mathbf{r})} \alpha.\sigma(\alpha) \leq \bigwedge_{\alpha \in \boldsymbol{f}(\mathbf{r})} \alpha.\tau(\alpha)\,.$$

From $\varphi(\mathbf{r}) \subseteq \mathbf{r}$ and by applying (Width),

$$\varphi_{\mathbf{r}} : \bigsqcap_{\alpha \in \varphi(\mathbf{r})} \alpha.\sigma(\alpha) \leq \bigsqcap_{\alpha \in \mathbf{r}} \alpha.\tau(\alpha) .$$

Let $\varphi' \stackrel{\text{def}}{=} \bigvee_{\tau \Downarrow \mathbf{r}} \varphi_{\mathbf{r}}$. From $\bigcup_{\tau \Downarrow \mathbf{r}} \varphi(\mathbf{r}') \cap \mathbf{r} = \varphi(\bigcup_{\tau \Downarrow \mathbf{r}} \mathbf{r}') \cap \mathbf{r} \subseteq \varphi(\mathbf{r})$ we observe that $\varphi' \wedge \bigwedge_{\alpha \in \mathbf{r}} \alpha.I(\tau(\alpha)) \quad \varphi_{\mathbf{r}}$. Hence, by (Weak), by iterating over all the ready sets of τ, and by (IChoice), we obtain

$$\varphi' : \bigoplus_{\tau \Downarrow \mathbf{r}} \bigsqcap_{\alpha \in \varphi(\mathbf{r})} \alpha.\sigma(\alpha) \leq \tau .$$

Now

$$\varphi' : \sigma \leq \bigoplus_{\tau \Downarrow \mathbf{r}} \bigsqcap_{\alpha \in \varphi(\mathbf{r})} \alpha.\sigma(\alpha)$$

by possibly applying (Must) for removing all the ready sets of σ that have disappeared in $\varphi(\tau)$ hence, by (Trans), we conclude $\varphi' : \sigma \leq \tau$. In order to prove $\varphi : \sigma \leq \tau$ it is sufficient to apply (Weak). This is possible because $\varphi \wedge I(\tau) \quad \varphi'$. Indeed, assume $\varphi(\tau) \xrightarrow{\alpha}$. Then $\alpha \in \mathbf{r}$ for some $\tau \Downarrow \mathbf{r}$, hence $\sigma \Downarrow \varphi(\mathbf{r})$ and now $\alpha \in \varphi(\mathbf{r})$. So, it must be $\varphi_{\mathbf{r}} \xrightarrow{\alpha}$ from which we conclude $\varphi' \xrightarrow{\alpha}$. □

3.4 Algorithmic deduction system

We introduced a device, filters, that allows us to transform a weak subcontract or compliance relation into a strong one by shielding the incompatible actions. The next step is to infer filters algorithmically, so that the weak relations can be used in practice.

As usual finding a decision algorithm for a containment relation corresponds to a cut-elimination process (the cut here being the (trans) rule in Table I), which amounts to finding a canonical proof for each provable relation. In other terms, we have to associate every provable weak subcontracting relation with a canonical filter that represents all other possible proofs. In order to choose a canonical filter, we have to solve two potential problems. First, there usually are several filters that work with a given relation. For example, to show that $a \oplus b \not\leq a + b$, we can either let pass only a, only b, or both. The best solution here is to let pass both, because we do not want to shield out actions that cannot cause any harm. This example suggests the definition of a notion of "better filter", that is, of a partial order on filters that determines which filter is better to use, and such partial order is exactly (Definition 3.12). The second problem is that in the example above a filter that lets a, b, and, say, c pass will work as well. The intuition here is that the filter that lets *just* a and b pass is better since the fact of allowing any action besides a and b is useless. This suggests the definitions of a notion of "filter relevance", to single out filters that do not contain useless actions.

The subcontracting algorithm will pick up, among all the possible filters for a given relation, the "best relevant" filter that proves it.

3.4.1 *Filter relevance.* In order to determine the property of "relevance" we have to better understand the role played by the identity filters we introduced in Definition 3.11. It may be noted that the identity filter of a given contract is exactly the tree (prefix-closed set of traces) of all possible sequences of actions that the contract can do before reducing to $\mathbf{0}$, without distinguishing between internal and external choices. This is embodied by the $\vee$ operator on filters which is a

unique choice operator representing both kinds of choice, as the following relation shows:

$$\boldsymbol{I}(\sigma \oplus \tau) = \boldsymbol{I}(\sigma + \tau) = \boldsymbol{I}(\sigma) \vee \boldsymbol{I}(\tau) \tag{2}$$

Note that if σ and τ share common actions in their outermost prefixes, the continuations of both filters after this action are correctly merged by the semantics of the disjunction operator.

The tree of an identity filter accurately represents the idea we mentioned in the introduction of a contract's "world": the sets of actions the contract knows of at each step of an interaction. Filter application can be seen as a *projection* of the contract onto the "world" represented by the filter. In the case of a relation $\boldsymbol{f} : \sigma \leq \tau$, $\boldsymbol{f}$ is used to restrict the "world" of τ: then the intuition is that in order to be relevant, $\boldsymbol{f}$ should be defined (only) on that world, which is represented by $\boldsymbol{I}(\tau)$. Indeed, applying to τ the filter $\boldsymbol{f}$ or the filter $\boldsymbol{f} \wedge \boldsymbol{I}(\tau)$ gives the same result, thus the part of $\boldsymbol{f}$ that is not in $\boldsymbol{f} \wedge \boldsymbol{I}(\tau)$ is irrelevant (and this is why there is no greatest filter corresponding to a given relation in the absolute). Thus we will say that a filter $\boldsymbol{f}$ is *relevant* with respect to a relation $\sigma \not\leq \tau$ if it is smaller than $\boldsymbol{I}(\tau)$ according to .

Now if we restrict ourselves to relevant filters we can have another interesting upper bound: by looking at condition (2) of the coinductive strong subcontract relation we see that, at each step, every action available in the greater contract has to be available also in the smaller one. This exactly means that the greater contract has a smaller tree, and thus we have (by noticing that $\boldsymbol{I}(\boldsymbol{f}(\sigma)) = (\boldsymbol{f} \wedge \boldsymbol{I}(\sigma))(\sigma)$):

$$\text{if } \sigma \subsetneq \boldsymbol{f}(\tau) \text{ and } \boldsymbol{f} \quad \boldsymbol{I}(\tau) \text{ then } \boldsymbol{f} \quad \boldsymbol{I}(\sigma) \tag{3}$$

Thus relevant filters that prove a relation have to be smaller than the identity filters of *both* contracts. This corresponds to the intuition that $\boldsymbol{f}$ embeds τ services into the "world" of σ: it projects them on something that is included in that world.

We now would like to find the greatest relevant filter that proves a given relation. Note that projecting on $\boldsymbol{I}(\sigma) \wedge \boldsymbol{I}(\tau)$ itself is not necessarily enough to make the relation work, because of ready sets: it might be necessary to project on something smaller to prevent a wrong branch to be taken. For example in $a \oplus b.(a + b) \not\leq a + b.(a \oplus b)$, the initial b has to be filtered out even if the trees are the same, because its continuation in the right contract has incompatible ready sets. However, the following important relation holds:

$$\text{if } \sigma \subsetneq \boldsymbol{f}(\tau) \text{ and } \sigma \subsetneq g(\tau) \text{ then } \sigma \subsetneq (\boldsymbol{f} \vee g)(\tau) \tag{4}$$

meaning that if we can make the relation work either by selecting some branches or by selecting some other branches, then it will still work if we take all these branches at once. This shows that, if $\sigma \not\leq \tau$ holds, there will be a greatest *subtree* of τ that makes the relation work: even if there is no greatest filter in the absolute, we can take the disjunction of all filters less than $\boldsymbol{I}(\tau)$ that work (there are a finitely many). This filter, which is the least upper bound of all relevant filters that prove $\sigma \not\leq \tau$, is the one we choose as canonical.

3.4.2 *Algorithm.* The last step is to define an algorithm for building the canonical filter of a relation. In this respect we have to solve two technical problems: the

Table III. Algorithmic deduction system for the weak subcontract relation.

$$\text{(a1)}\quad \frac{(\sigma,\tau)\in\Gamma}{\Gamma \;\emptyset : \sigma \;\; \tau}$$

$$\text{(a2)}\quad \frac{\forall s\in R(\tau) : s\cap a\in R(\sigma) \qquad a=\{\alpha\in \mathrm{init}(\sigma)\cap \mathrm{init}(\tau) \mid \exists F_\alpha : \Gamma\cup\{(\sigma,\tau)\} \;\; F_\alpha : \sigma(\alpha) \;\; \tau(\alpha)\}}{\Gamma \;\; \bigcup_{\alpha\in a} F_\alpha \cup \{(\sigma,\tau) \xrightarrow{1} a\} : \sigma \;\; \tau}$$

first problem is due to the fact that, although the algorithm works on infinite terms, it must always be able to report success or failure in finite time. Since contracts are assumed to be regular, we use the well-known technique of memoization for recording pairs of contracts that we deem related, so that they are not processed if found again. To this end we equip judgments with a context Γ storing pairs of contracts already examined. The second problem regards the computation of the canonical filter that proves a relation: it is clear that, in general, such a filter will not be finite and nonetheless we currently have no finite representation for filters. However, a filter is nothing but the specification, at any given time during an interaction, of a (finite) set of actions that are not shielded, namely the set a in Definition 3.1. In particular, because of the regularity of the contracts being related, the set of such a's is necessarily finite. From this set of a's it is trivial to produce a possibly infinite, regular filter. We use F to range over (finite) maps from pairs of contracts to finite sets of actions. For any given contracts σ and τ such that $\sigma \not\simeq \tau$, the algorithm infers a map F, defined on every pair (σ', τ') reachable from (σ, τ) after some sequence of interactions, which associates with such a pair the finite set of actions a that are not shielded at that point.

Definition 3.18. *We define the relation $\Gamma \vdash F : \sigma ::: \tau$ by the inference rules in Table III. We write $F : \sigma ::: \tau$ for $\emptyset \vdash F : \sigma ::: \tau$.*

Rule (a1) applies when the contracts being processed have already been encountered and assumed to be related. In this case the inferred map F is empty, because the set a of actions that need not be shielded for relating σ and τ is already computed by the instance of the rule where σ and τ occurred for the first time. In rule (a2), the set a represents the largest set of actions leading to continuations which are in the relation, namely a is the largest set of (relevant) actions that need not be shielded for two contracts to be related. The condition on the first line requires a to be large enough, so that when τ is restricted to the actions in a, τ manifests a behavior that is (more deterministic than) that of σ.

It is trivial to see that if F is synthesized by the algorithm and $\{(\sigma', \tau') \xrightarrow{1} a, (\sigma', \tau') \xrightarrow{1} a'\} \subseteq F$, then we have $a = a'$. Hence F is indeed a map and from now on we will write $F(\sigma, \tau)$ for the set a associated with (σ, τ) in F. Additionally, $F : \sigma ::: \tau$ implies the following properties

(1) $(\sigma, \tau) \in \mathrm{dom}(F)$;

(2) $(\sigma^l, \tau^l) \in \mathrm{dom}(F)$ and $\alpha \in F(\sigma^l, \tau^l)$ implies $(\sigma^l(\alpha), \tau^l(\alpha)) \in \mathrm{dom}(F)$.

Overall if $F : \sigma ::: \tau$, then the map F represents the (possibly infinite) filter $F[\sigma, \tau]$ defined by the equation

$$F[\sigma, \tau] = \bigvee_{\alpha \in F(\sigma,\tau)} \alpha.F\,[\sigma(\alpha),\ \tau(\alpha)]\ .$$

The regularity of such filter is a direct consequence of the regularity of σ and τ while contractivity stems from the finiteness of the init(σ) and init(τ) sets (thus of the α's) and from the construction of $F[\sigma, \tau]$.

Remark 3.19. *The rule* (a2) *in Table III is more an algorithmic specification than a deduction rule, insofar as it describes how to compute the set* a*, rather than how to build a proof tree. The following rule*

$$\text{(a2)}\qquad \frac{\forall \alpha \in a \quad \Gamma \cup \{(\sigma,\tau)\} \vdash F_\alpha : \sigma(\alpha) ::: \tau(\alpha) \qquad \forall \beta \in (\mathrm{init}(\sigma) \cap \mathrm{init}(\tau)) \not\in a}{\Gamma \vdash \bigcup_{\alpha \in a} F_\alpha \cup \{(\sigma,\tau)\ 1 \to a\} : \sigma ::: \tau} \quad \begin{array}{l} \Gamma \cup \{(\sigma,\tau)\} \quad F : \sigma(\beta)\ \ \tau(\beta) \\ \forall s \in R(\tau) : s \cap a \in R(\sigma) \end{array}$$

is its proof theoretic counterpart.

3.4.3 *Properties.* The algorithm described in Definition 3.18 enjoys fundamental properties, namely **(*i*)** it proves only (soundness) and all (completeness) weak subcontract relations, **(*ii*)** in case of success it returns the largest relevant filter that proves the relation and **(*iii*)** it always terminates, which implies the decidability of the weak subcontract relation.

Lemma 3.20 **filter relevance**. *If $F : \sigma ::: \tau$, then $F[\sigma, \tau]$ $I(\tau)$.*

Proof. By definition of $F[\sigma, \tau]$ it is trivial to verify that $F[\sigma, \tau] \xrightarrow{\phi}$ implies $\tau \xrightarrow{\phi}$, from which relevance follows immediately. □

Before proving soundness, we need an auxiliary (cut-elimination) result stating that an hypothesis $\sigma \not\subseteq \tau$ that is necessary for proving $\sigma' \not\subseteq \tau'$ can be discharged if $\sigma \not\subseteq \tau$ is itself provable.

Proposition 3.21. *If (1) $\Gamma \vdash F : \sigma ::: \tau$ and (2) $\Gamma \cup \{(\sigma,\tau)\} \vdash F' : \sigma' ::: \tau'$, then there exists F'' such that $F' \subseteq F''$ and $\Gamma \vdash F'' : \sigma' ::: \tau'$.*

Proof. We reason by induction on the derivation tree of (2) and by cases on the last rule applied. Assume the last rule was (a1). Then $(\sigma', \tau') \in \Gamma \cup \{(\sigma,\tau)\}$ and $F' = \emptyset$. We distinguish two subcases: if $(\sigma', \tau') \in \Gamma$, then we conclude immediately by (a1) and by taking $F'' = \emptyset$; if $\sigma' \equiv \sigma$ and $\tau' \equiv \tau$, then we conclude by hypothesis (1) and by taking $F'' = F$. Assume the last rule was (a2) and let a be the set determined in the premises of the rule. For every $\alpha \in a$ we have that there exists F_α such that $\Gamma' \cup \{(\sigma,\tau)\} \vdash F_\alpha : \sigma'(\alpha) ::: \tau'(\alpha)$ where $\Gamma' = \Gamma \cup \{(\sigma', \tau')\}$ and $F' = \bigcup_{\alpha \in a} F_\alpha \cup \{(\sigma', \tau')\ 1 \to a\}$. From (1) and $\Gamma \subseteq \Gamma'$ we derive $\Gamma' \vdash F : \sigma ::: \tau$. By induction hypothesis there exists F'_α such that $F_\alpha \subseteq F'_\alpha$ and $\Gamma' \vdash F'_\alpha : \sigma'(\alpha) ::: \tau'(\alpha)$ for every $\alpha \in a$. Hence we can apply rule (a2) and conclude that $\Gamma \vdash F'' : \sigma' ::: \tau'$ where $F'' = \bigcup_{\alpha \in a} F'_\alpha \cup \{(\sigma', \tau')\ 1 \to a\}$, observing that $F' \subseteq F''$. □

Theorem 3.22 (soundness). *If $F : \sigma ::: \tau$ then $\sigma \leq F[\sigma, \tau](\tau)$.*

Proof. We prove that $S \stackrel{\text{def}}{=} \{(\sigma, F[\sigma, \tau](\tau)) \mid F : \sigma ::: \tau\}$ is a coinductive strong subcontract relation. Let $(\sigma, \tau') \in S$, then there exist F and τ such that $F : \sigma ::: \tau$ and $\tau' \equiv F[\sigma, \tau](\tau)$. As regards condition 1 in the definition of coinductive strong

subcontract relation, let $\tau \Downarrow s$. Then $F[\sigma,\tau](\tau) \Downarrow s \cap F(\sigma,\tau)$ and from $s \cap F(\sigma,\tau) \in R(\sigma)$ we conclude that there exists $\mathbf{r}$ such that $\sigma \Downarrow \mathbf{r}$ and $\mathbf{r} \subseteq s \cap F(\sigma,\tau)$. As regards condition 2, assume $F[\sigma,\tau](\tau) \xrightarrow{\alpha}$. By definition of $F[\sigma,\tau]$ we also have $\sigma \xrightarrow{\alpha}$ and, for every $\alpha \in F(\sigma,\tau)$, there exists F_α such that $\{(\sigma,\tau)\}\ t\text{-}\ F_\alpha : \sigma(\alpha) ::: \tau(\alpha)$. By Proposition 3.21 there exists F'_α such that $F_\alpha \subseteq F'_\alpha$ and $F'_\alpha : \sigma(\alpha) ::: \tau(\alpha)$. Notice also that $F'_\alpha \subseteq F$ since the former proves $\sigma(\alpha) ::: \tau(\alpha)$, the latter $\sigma ::: \tau$, and by the uniqueness of the filters derived by the algorithm F'_α must correspond to $(\alpha)) \in S$ by observing that $\tau'(\alpha) \equiv F[\sigma,\tau](\tau)(\alpha) \equiv F'_\alpha[\sigma(\alpha), \tau(\alpha)](\tau(\alpha))$ and by definition of S. □

Theorem 3.23 (completeness). *If $\sigma \leq g(\tau)$, then there exists F such that $F : \sigma ::: \tau$, and $F[\sigma,\tau] \quad g \wedge \mathbb{1}(\tau)$.*

Proof. First note that if $\sigma \leq g(\tau)$, then also $\sigma \leq (g \wedge \mathbb{1}(\tau))(\tau)$ (applying the conjunction of two filters is like applying one then the other, it projects on the part of the tree common to both), thus we can assume $g \quad \mathbb{1}(\tau)$ without loss of generality.

The theorem is stated for a memoization environment $\Gamma = \emptyset$ (recall that $F : \sigma ::: \tau$ stands for $\emptyset\ t\text{-}\ F : \sigma ::: \tau$ and that a memoization environment is a finite set of pairs of contracts). To integrate memoization environments in our proof we generalize the statement and prove that if $\sigma \leq g(\tau)$ and $g \quad \mathbb{1}_\tau$, then for all Γ:

(1) there exists F such that $\Gamma\ t\text{-}\ F : \sigma ::: \tau$;

(2) $(\sigma,\tau) \not\in \Gamma \Rightarrow \mathrm{init}(g) \subseteq F(\sigma,\tau)$;

Completeness then follows immediately from (1) by taking $\Gamma = \emptyset$, and maximality of the inferred filter is easily deduced from (2).

Let $R(\Gamma, \sigma, \tau) \stackrel{\text{def}}{=} \{(\sigma(\phi), \tau(\phi)) \mid \sigma \xrightarrow{\phi}, \tau \xrightarrow{\phi}\} \setminus \Gamma$, and note that by regularity of σ and τ, the set is finite. We can thus reason by induction on $R(\Gamma, \sigma, \tau)$ to show the more general property.

Assume $(\sigma,\tau) \in \Gamma$. Note that if $R(\Gamma, \sigma, \tau) = \emptyset$ this is the only possible case. Then we conclude immediately by rule (a1) and by taking $F = \emptyset$. Assume $(\sigma,\tau) \not\in \Gamma$ and let $\Gamma' \stackrel{\text{def}}{=} \Gamma \cup \{(\sigma,\tau)\}$. Suppose $g(\tau) \xrightarrow{\alpha}$. From the hypothesis $\sigma \leq g(\tau)$ we derive $\sigma \xrightarrow{\alpha}$ and $\sigma(\alpha) \leq g(\alpha)(\tau(\alpha))$. We have $R(\Gamma', \sigma(\alpha), \tau(\alpha)) \subsetneq R(\Gamma, \sigma, \tau)$ because (σ,τ) is in the latter and not in the former, hence by induction hypothesis there exists F_α such that $\Gamma'\ t\text{-}\ F_\alpha : \sigma(\alpha) ::: \tau(\alpha)$. We can do this for any α such that $g(\tau) \xrightarrow{\alpha}$, thus because of the hypothesis that $g \quad \mathbb{1}_\tau$ we have that the set a in the premises of rule (a2) is such that $\mathrm{init}(g) \subseteq a$. Therefore the F appearing in the conclusion of that rule satisfies property (2) and we just have to check that the condition on the first line of the premises is satisfied. Let $s \in R(\tau)$. It contains a ready set s' of τ. Since $\sigma \leq g(\tau)$, there exists $\mathbf{r} \subseteq s' \cap \mathrm{init}(g)$ such that $\sigma \Downarrow \mathbf{r}$. As $\mathrm{init}(g)$ is included in a and s' in s, we also have $\mathbf{r} \subseteq s \cap a$. Then $s \cap a \in R(\sigma)$, because a is included in $\mathrm{init}(\sigma)$ by definition. □

Corollary 3.24. *If σ and τ are two contracts, there exists at most one F such that $F : \sigma ::: \tau$. Furthermore, if $F : \sigma ::: \tau$, then*

$$F[\sigma,\tau] = \max\{g \quad \mathbb{1}(\tau) \mid \sigma \leq g(\tau)\} = \max\{g \quad \mathbb{1}(\tau) \mid g : \sigma \leq \tau\}.$$

The corollary above describes the logical interpretation of the algorithm as the result of a cut-elimination process. The "cut" in the system of Table I is given by the rule (trans). This rule intersects filters, that is it minimizes the proofs: therefore in order to eliminate cuts we have to find a proof with a maximum filter. However we have also to avoid useless applications of the (weak) rule, which instead maximizes proofs: therefore we have to set an upper bound to filter maximization, which is embodied by the definition of relevance (therefore it would be more precise to speak of a cut-weakening-elimination process).

Proposition 3.25 (decidability). *Given two contracts σ and τ, we can decide whether there exists F such that $F : \sigma ::: \tau$.*

Proof. Trivial consequence of the regularity of σ and τ. □

4. PROCESSES

In this section we relate contracts (which are behavioral types) with processes that implement clients and services. We do not consider any particular process language, nor do we require that clients and services be implemented using the same language. We just require that the observable behavior of processes be described by a labeled transition system and abstracted by a static type system. More precisely we assume that a process language is equipped with a labeled transition system so that

$$P \xrightarrow{\mu} P'$$

describes the evolution of a process P that performs a μ action thus becoming the process P'. Here, μ can either be a visible action of the form a or $\bar{a}$, which is meant to synchronize with the corresponding co-action in the process P is interacting with, or it can be an internal, invisible action τ (not to be confused with τ that we used to range over contracts) that the process P executes autonomously. It is understood that the relation $\xrightarrow{\mu}$ is not necessarily deterministic. As usual, we let α range over visible actions and we write $P \xrightarrow{\mu}$ if $P \xrightarrow{\mu} P'$ for some process P'. Also, we say that P *diverges* if there exists an infinite sequence $P_0, P_1, \ldots$, such that $P = P_0 \xrightarrow{\tau} P_1 \xrightarrow{\tau} \cdots$.

Definition 4.1 (strong process compliance). *Let $P \mid Q \longrightarrow P' \mid Q'$ be the least relation defined by the rules:*

$$\frac{P \xrightarrow{\tau} P'}{P \mid Q \longrightarrow P' \mid Q} \qquad \frac{Q \xrightarrow{\tau} Q'}{P \mid Q \longrightarrow P \mid Q'} \qquad \frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{\alpha}} Q'}{P \mid Q \longrightarrow P' \mid Q'}$$

We write $\Longrightarrow$ for the reflexive, transitive closure of $\longrightarrow$; we write $P \mid Q \longrightarrow$ if $P \mid Q \longrightarrow P' \mid Q'$ for some P' and Q'; we write $P \mid Q \not\longrightarrow$ if not $P \mid Q \longrightarrow$. A computation of $P \mid Q$ is a sequence $P \mid Q = P_0 \mid Q_0 \longrightarrow P_1 \mid Q_1 \longrightarrow \cdots$. A computation of $P \mid Q$ is maximal if either it is infinite or there exists $P_n \mid Q_n$ such that $P \mid Q \Longrightarrow P_n \mid Q_n \not\longrightarrow$.

The client P is strongly compliant *with the service Q, written P -- Q, if for every configuration $P_i \mid Q_i$ of every maximal computation there exists $j \geq i$ such that either $P_j \xrightarrow{\alpha} P_{j+1}$ for some α or $P_j \not\xrightarrow{\tau}$ and $P_j \xrightarrow{e}$.*

The intuition of this definition is that $P \mid Q$ represents a client P and a service Q interacting with each other. When $P \dashv Q$ every interaction between P and Q is such that either P and Q interact infinitely often, or the client invariably reaches a state in which it is able to emit e, denoting the successful completion of P's task.

We also assume that a type system is given to check that a process P *implements* the contract σ. This is expressed by the judgment

$$t \vdash P : \sigma$$

While we do not give details on the particular typing rules, we require typing and the reduction relation to satisfy some basic properties: essentially, contracts must describe the observational behavior of processes and reduction must decrease non-determinism (entropy must always increase). In this respect, it makes sense to be able to apply the strong subcontract relation to client contracts too, where the action e is treated like any other action (recall that, according to Theorem 2.9, the relation $\subsetneq$ can be defined without any notion of "successful action" e).

Definition 4.2. *The type system is* consistent *if, whenever* $t \vdash P : \sigma$*, we have*

(1) $P \xrightarrow{\tau} P'$ *implies* $t \vdash P' : \sigma'$ *and* $\sigma \subsetneq \sigma'$;

(2) $P \xrightarrow{\alpha} P'$ *implies* $t \vdash P' : \sigma'$, $\sigma \xrightarrow{\alpha}$, *and* $\sigma(\alpha) \subsetneq \sigma'$;

(3) P *diverges implies* $\sigma \Downarrow \emptyset$;

(4) $P \not\xrightarrow{\tau}$ *implies* $\sigma \Downarrow \mathbf{r}$ *and* $\mathbf{r} \subseteq \{\alpha \mid P \xrightarrow{\alpha}\}$.

Intuitively, condition (1) states that a process performing internal actions can only make its contract more deterministic. Condition (2) states that if a process performs a visible action α, then its contract must account for that action and the contract of the resulting process P' is (more deterministic than) the contract $\sigma(\alpha)$, which accounts for all the possible behaviors of P after α. Condition (3) states that a divergent process may be observationally invisible, namely its contract must account for an empty ready set (the process may never be "ready" to perform any action). Finally, condition (4) states that the contract of a stable process should have at least one ready set that provides no more capabilities than those of the process.

The following lemma states that it is possible to replace a client contract ρ with another one which is more deterministic, still preserving the compliance property. The lemma is fundamental in proving the soundness of the type system.

Lemma 4.3. *If* $\rho \dashv \sigma$ *and* $\rho \subsetneq \rho'$ *then* $\rho' \dashv \sigma$.

Proof. Let $\mathcal{C}$ be a compliance relation such that $(\rho, \sigma) \in \mathcal{C}$ and let $\mathcal{S}$ be a strong subcontract relation such that $(\rho, \rho') \in \mathcal{S}$. It is sufficient to prove that

$$\mathcal{C}' \stackrel{\text{def}}{=} \{(\rho', \sigma) \mid \exists \rho : (\rho, \sigma) \in \mathcal{C} \wedge (\rho, \rho') \in \mathcal{S}\}$$

is a strong compliance relation. Assume $(\rho', \sigma) \in \mathcal{C}'$. Then there exists ρ such that $(\rho, \sigma) \in \mathcal{C}$ and $(\rho, \rho') \in \mathcal{S}$. As regards condition (1) in Definition 2.6, assume $\rho' \Downarrow \mathbf{r}$ and $\sigma \Downarrow s$. If $e \in \mathbf{r}$, then the condition is satisfied. Assume $e \,;\in \mathbf{r}$. From $(\rho, \rho') \in \mathcal{S}$ there exists $\mathbf{r}' \subseteq \mathbf{r}$ such that $\rho \Downarrow \mathbf{r}'$. In particular, $e \,;\in \mathbf{r}'$. From $(\rho, \sigma) \in \mathcal{C}$ we have $\mathrm{co}(\mathbf{r}') \cap s \,;= \emptyset$, hence $\mathrm{co}(\mathbf{r}) \cap s \,;= \emptyset$.

As regards condition (2) in Definition 2.6, assume $\rho' \xrightarrow{\alpha}$ and $\sigma \xrightarrow{\alpha}$. From $(\rho, \rho') \in S$ we derive $\rho \xrightarrow{\alpha}$ and $(\rho(\alpha), \rho'(\alpha)) \in S$. From $(\rho, \sigma) \in C$ we derive $(\rho(\alpha), \sigma(\alpha)) \in C$. Hence we conclude $(\rho'(\alpha), \sigma(\alpha)) \in C'$ by definition of C'. □

Given a consistent type system, the following result states that, given a pair of processes $P \quad Q$ whose respective contracts comply, and given any two residual processes $P' \quad Q'$ resulting from $P \quad Q$, the respective contracts of P' and Q' comply as well.

Lemma 4.4 (subject reduction). *If τ- $P : \rho$ and τ- $Q : \sigma$ and ρ -- σ and $P \quad Q \longrightarrow P' \quad Q'$, then τ- $P' : \rho'$ and τ- $Q' : \sigma'$ and ρ' -- σ'.*

Proof. We need to consider all the possibilities by which $P \quad Q$ reduces to $P' \quad Q'$, namely $P \quad Q \longrightarrow P' \quad Q'$. If $P \xrightarrow{\tau} P'$, then from consistency condition (1) we have τ- $P' : \rho'$ and $\rho \subsetneq \rho'$ and by Lemma 4.3 we conclude ρ' -- σ. If $Q \xrightarrow{\tau} Q'$, then from consistency condition (1) we have τ- $Q' : \sigma'$ and $\sigma \subsetneq \sigma'$ and by definition of $\subsetneq$ we conclude ρ -- σ'. Finally, if $P \xrightarrow{\alpha} P'$ and $Q \xrightarrow{\alpha} Q'$, then from consistency condition (2) we have that τ- $P' : \rho'$ and τ- $Q' : \sigma'$ and $\rho(\alpha) \subsetneq \rho'$ and $\sigma(\alpha) \subsetneq \sigma'$. By Lemma 4.3 and by definition of $\subsetneq$ we conclude ρ' -- σ'. □

The soundness of a consistent type system is ensured by the following result, stating that if the contracts of two processes comply, the corresponding processes comply as well, guaranteeing that either the two processes synchronize infinitely many times or the client successfully terminates.

Theorem 4.5. *If τ- $P : \rho$ and τ- $Q : \sigma$ and ρ -- σ then P -- Q.*

Proof. Because of Lemma 4.4 we only need to consider the cases when $P \quad Q \not\Downarrow$ or $P \not\Downarrow$ and Q diverges. Indeed, from ρ -- σ we derive that $\rho \Downarrow \mathbf{r}$ implies $\mathbf{r} \neq \emptyset$, hence P cannot diverge, for otherwise we would have $\rho \Downarrow \emptyset$ by consistency condition (3). Let now $P \quad Q \longrightarrow$ and assume, by contradiction, that $P \not\xrightarrow{e}$. From $P \quad Q \longrightarrow$ we have that whenever $P \xrightarrow{\alpha}$ we have $Q \not\xrightarrow{\overline{\alpha}}$. From consistency condition (4) there exist $\mathbf{r}$ and s such that $\rho \Downarrow \mathbf{r}$ and $\sigma \Downarrow$ s and $\mathrm{co}(\mathbf{r}) \cap$ s $= \emptyset$ and $e \in \mathbf{r}$, but this is absurd from the hypothesis that ρ -- σ. Hence $P \xrightarrow{e}$. Assume that $P \longmapsto$ and Q diverges. By consistency condition (3) we derive $\sigma \Downarrow \emptyset$, hence $\rho \Downarrow \mathbf{r}$ implies $e \in \mathbf{r}$. From consistency condition (4) we conclude $P \xrightarrow{e}$. □

The soundness theorem holds when the client's contract and the service's contract are strongly compliant. To be able to use a service for which we only have a weakly compliant client, we need to shield potentially dangerous service actions by means of a filter. Thus, we enrich the process language with an operator

$$\boldsymbol{f}[P]$$

that applies a filter $\boldsymbol{f}$ to a process P, the idea being that the filter constraints the set of visible actions of P, that is its capabilities to interact with the environment, still not altering its ability to evolve autonomously. The labeled transition system

of the language is consequently enriched with the following two inference rules:

$$\frac{P \xrightarrow{\alpha} P' \qquad f \xrightarrow{\alpha} f'}{f[P] \xrightarrow{\alpha} f'[P']}\ (\text{Filter1}) \qquad \frac{P \xrightarrow{\mathbf{t}} P'}{f[P] \xrightarrow{\mathbf{t}} f[P']}\ (\text{Filter2})$$

The introduction of filters into the process language has consequences on the type system as well. Since our discussion is parametric in the process language and in the type system, we only need to show that the typing rule

$$\frac{t\text{-}P : \sigma}{t\text{-}f[P] : f(\sigma)}\ (\text{TypeFilter})$$

preserves the consistency of the type system.

Proposition 4.6. *A consistent type system enriched with rule* (TypeFilter) *results in another consistent type system.*

Proof. Let $t\text{-}P : \sigma$. As regards consistency condition (1), assume $P \xrightarrow{\mathbf{t}} P'$ and $t\text{-}P : \sigma'$. Then $\sigma \leq \sigma'$ implies $f(\sigma) \leq f(\sigma')$ by Proposition 3.8. As regards consistency condition (2), assume that $P \xrightarrow{\alpha} P'$ and $t\text{-}P' : \sigma'$. There are two possibilities: if $f \not\xrightarrow{\alpha}$, then $f[P] \not\xrightarrow{\alpha}$ and there is nothing to prove. If $f \xrightarrow{\alpha} f'$, then $\sigma(\alpha) \leq \sigma'$. Now we conclude $f(\sigma)(\alpha) = f'(\sigma(\alpha)) \leq f'(\sigma')$. As regards consistency condition (3), assume that $f[P]$ diverges. Then P diverges and we must have $\sigma \Downarrow \emptyset$. We immediately conclude $f(\sigma) \Downarrow \emptyset$. Finally, as regards consistency condition (4), assume that $f[P] \not\xrightarrow{\mathbf{t}}$. Then $P \not\xrightarrow{\mathbf{t}}$. We derive $\sigma \Downarrow \mathbf{r}$ where $\mathbf{r} \subseteq \{\alpha \mid P \xrightarrow{\alpha}\}$, hence $f(\sigma) \Downarrow f(\mathbf{r})$ and we conclude by observing that $f(\mathbf{r}) \subseteq \{\alpha \mid f[P] \xrightarrow{\alpha}\}$. □

The following result summarizes the contribution of our work: the adoption of filters enlarges the number of services that satisfy a client.

Corollary 4.7. *If* $t\text{-}P : \rho$, $t\text{-}Q : \sigma$, *and* $\rho \text{ -- } f(\sigma)$, *then* $P \text{ -- } f[Q]$.

5. PRACTICE OF CONTRACTS

Hitherto we developed our theory by working on infinite trees, for both types and filters. The main advantage of this approach is that the resulting theory does not depend on a particular concrete syntax used to finitely denote infinite trees. Of course, the use of infinite trees is infeasible in practice and as soon as one wants to devise typing systems and algorithms for actual languages (or just process calculi) it is necessary to introduce a concrete finite syntax to denote possibly infinite trees. Remarkably, the results stated for infinite trees easily carry over to whatever (reasonable) concrete syntax we choose to denote them, by using classic techniques dating back to Bruno Courcelle's seminal work [Courcelle 1983]. This contrasts with the fact that transposing the results stated for one syntax onto another can be quite hard, since one has to sieve the properties that hold for infinite trees from those that are meaningful only for the particular syntax at issue, whence the interest of our approach.

Choosing a particular concrete syntax neither is without consequences nor is it just a matter of taste. Two concrete syntaxes are quite popular in the process

algebras literature: the first one uses explicit recursion variables while the second uses the Kleene star to denote an unbound number of occurrences of some subtree. Each of them fits different applications. In the rest of this section we first introduce these two concrete syntaxes and we show how the main properties we studied in the previous sections for infinite trees (compliance, subcontracting, ...) transpose to them. Next we apply each syntax them to a Web service description language: we show that wscl diagrams (§2.2) can be straightforwardly encoded by resorting to recursion variables and that ws-bpel so-called activities can be naturally typed using Kleene notation. In this latter case, we define a contract based type system and, above all, show how to use filters to trim down the case explosion introduced by the use of parallel compositions of activities.

> **Terminology.** In the rest of this section we introduce the two concrete syntaxes for contracts and filters we hinted above: the one based on recursive variables and the other on Kleene's stars. In order not to clutter the notation, in the concrete syntax we will use the same metavariables for contracts and filters that we used for the corresponding possibly infinite terms of the previous sections. To avoid any ambiguity we will use the terminology *unfolded* contract/filter when referring to the possibly infinite terms used so far, *recursive* contract/filter for terms generated by using explicit recursion variables, and *regular* contract/filter for terms using the Kleene star. We will omit the qualifying adjectives only when no confusion can arise.

5.1 Concrete syntax for contracts

The first concrete syntax for regular contracts is the same as given in §2.1 for unfolded contracts/terms, extended with the well-known recursion operator $\text{rec}\, x = \sigma$ which binds the *recursion variable* x in σ. The idea is that an occurrence of x in σ stands for the whole $\text{rec}\, x = \sigma$ term. A *recursive contract* is a finite term generated by the following grammar:

$$\sigma ::= \mathbf{0} \mid a.\sigma \mid \sigma + \sigma \mid \sigma \oplus \sigma \mid \text{rec}\, x = \sigma \mid x$$

Similarly a *recursive filter* is a finite term inductively generated by the grammar

$$\boldsymbol{f} ::= \mathbf{0} \mid a.f \mid \boldsymbol{f} \vee \boldsymbol{f} \mid \boldsymbol{f} \wedge \boldsymbol{f} \mid \text{rec}\, x = \boldsymbol{f} \mid x$$

As usual we write $\text{fv}(\sigma)$ and $\text{bv}(\sigma)$ for denoting the free and the bound variables occurring in σ, respectively (their definition is standard); we say that σ is *closed* if $\text{fv}(\sigma) = \emptyset$; we write $\sigma\{\tau/x\}$ for the contract obtained from σ by replacing every free occurrence of x with τ; we proceed similarly for filters. Using this syntax, contractivity corresponds to requiring that in a subterm $\text{rec}\, x = \sigma$ (respectively, $\text{rec}\, x = \boldsymbol{f}$) every free occurrence of x in σ (respectively, in $\boldsymbol{f}$) be guarded by at least one prefix. Thus we rule out terms such as e.g. $\text{rec}\, x = x + x$ or $\text{rec}\, x = x \vee x$.

Intuitively, every recursive contract corresponds to the (possibly infinite) unfolded contract obtained by repeatedly unfolding every $\text{rec}\, x = \sigma$ to $\sigma\{\text{rec}\, x = \sigma/x\}$ (and similarly for filters). Consequently, the semantics of a term above is equal to the semantics of the infinite tree it denotes. More rigorously, let a *system of regular equations* be a finite set $\{x_1 = \sigma_1, \ldots, x_n = \sigma_n\}$ of equations where $x_1, \ldots, x_n$ are

the *unknowns* and $\sigma_1, \ldots, \sigma_n$ are recursive contracts such that $\mathrm{fv}(\sigma_i) \subseteq \{x_1, \ldots, x_n\}$ for every $1 \le i \le n$. We associate each closed recursive contract with a pair (E, x) where E is a system of regular equations and x one of its unknowns called the *initial unknown*. If the σ_i's of E are such that every free occurrence of a variable is guarded by at least a prefix, then the system of equations satisfies the so-called Greibach condition [Courcelle 1983] and, by Theorem 4.3.1 of [Courcelle 1983], the system admits a unique solution of unfolded contracts $(\tau_1, \ldots, \tau_n)$ such that $\tau_i = \sigma_i\{\tau_1/x_1\} \cdots \{\tau_n/x_n\}$ for every $1 \le i \le n$. Then, we define the semantics of a closed recursive contract as the τ_i component corresponding to the initial unknown associated with it.

Let σ be a closed recursive contract such that $\mathrm{bv}(\sigma) = \{x_1, \ldots, x_n\}$. Without loss of generality, assume that every x_i is bound exactly once in σ. Let $E(\sigma)$ be the function inductively defined by the rules:

$$E(\mathbf{0}) = \mathbf{0} : \emptyset \qquad E(x) = x : \emptyset \qquad \frac{E(\sigma) = \sigma' : E}{E(a.\sigma) = a.\sigma' : E}$$

$$\frac{E(\sigma) = \sigma' : E \quad E(\tau) = \tau' : E'}{E(\sigma + \tau) = \sigma' + \tau' : E \cup E'} \qquad \frac{E(\sigma) = \sigma' : E \quad E(\tau) = \tau' : E'}{E(\sigma \oplus \tau) = \sigma' \oplus \tau' : E \cup E'}$$

$$\frac{E(\sigma) = \sigma' : E \quad x \not\in \mathrm{fv}(\sigma)}{E(\mathrm{rec}\, x = \sigma) = \sigma' : E} \qquad \frac{E(\sigma) = \sigma' : E \quad x \in \mathrm{fv}(\sigma)}{E(\mathrm{rec}\, x = \sigma) = x : E \cup \{x = \sigma'\}}$$

The pair composed of the system of regular equations and the initial unknown associated with σ, denoted by $\mathrm{R}(\sigma)$, is defined as follows:

$$\mathrm{R}(\sigma) \stackrel{\text{def}}{=} \begin{array}{ll} (E, x_i) & \text{if } E(\sigma) = x_i : E \\ (E \cup \{x_0 = \sigma'\}, x_0) & \text{otherwise} \end{array}$$

The semantics $[\![\sigma]\!]$ of the recursive contract σ is the unfolded contract τ_i, where $(\tau_0, \tau_1, \ldots, \tau_n)$ is the unique solution of the system E such that $\mathrm{R}(\sigma) = (E, x_i)$.

The following proposition formalizes the fact that a recursive contract $\mathrm{rec}\, x = \sigma$ and its unfolding $\sigma\{\mathrm{rec}\, x = \sigma/x\}$ are equivalent, namely that they are associated with the same regular system and hence they denote the same regular contract.

Proposition 5.1. *Let* $E(\mathrm{rec}\, x = \sigma) = x : E \cup \{x = \sigma'\}$. *Then* $E(\sigma\{\mathrm{rec}\, x = \sigma/x\}) = \sigma' : E \cup \{x = \sigma'\}$.

Proof. We prove a more general statement. Let $\mathrm{dom}(E)$ be the set of unknowns in a regular system E; let $E\{\tau/x\} \stackrel{\text{def}}{=} \{y = \sigma\{\tau/x\} \mid x = \sigma \in E\}$, where we assume that $\mathrm{dom}(E) \cap \mathrm{fv}(\tau) = \emptyset$; let σ and τ be two contracts such that $\mathrm{bv}(\sigma) \cap \mathrm{fv}(\tau) = \emptyset$. We prove that if $x \in \mathrm{fv}(\sigma)$, then $E(\sigma\{\tau/x\}) = \sigma'\{\tau'/x\} : E\{\tau'/x\} \cup F$, where $E(\sigma) = \sigma' : E$ and $E(\tau) = \tau' : F$. If this holds, the proposition follows immediately by posing $\tau = \mathrm{rec}\, x = \sigma$. Indeed, if $x \not\in \mathrm{fv}(\sigma)$, then $E(\tau) = E(\sigma) = E(\sigma\{\tau/x\})$. On the other hand, if $x \in \mathrm{fv}(\sigma)$, then $E(\sigma\{\tau/x\}) = \sigma'\{x/x\} : E\{x/x\} \cup E \cup \{x = \sigma'\}$ and we conclude immediately since $\sigma'\{x/x\} \equiv \sigma'$ and $E\{x/x\} = E$.

As regards the more general statement, we prove it by induction on σ (recall that σ is a recursive contract, hence it is finite).

($\sigma \equiv \mathbf{0}$). Trivial since $x \not\in \mathrm{fv}(\sigma)$.

($\sigma \equiv x$). We have $\sigma' \equiv x$ and $E = \emptyset$. Now $E(\sigma\{\tau/x\}) = E(\tau) = \tau' : F$ and we conclude by observing that $\sigma'\{\tau'/x\} \equiv \tau'$ and $E\{\tau'/x\} = \emptyset$.

($\sigma \equiv y$, $y \neq x$). Trivial since $x \not\in \mathrm{fv}(\sigma)$.

($\sigma \equiv \alpha.\sigma_1$). We have $\sigma' \equiv \alpha.\sigma'_1$, where $E(\sigma_1) = \sigma'_1 : E$. From $x \in \mathrm{fv}(\sigma)$ we deduce $x \in \mathrm{fv}(\sigma_1)$, hence by induction hypothesis we derive $E(\sigma_1\{\tau/x\}) = \sigma'_1\{\tau'/x\} : E\{\tau'/x\} \cup F$. Now $E(\sigma\{\tau/x\}) = E(\alpha.\sigma_1\{\tau/x\}) = \alpha.\sigma'_1\{\tau'/x\} : E\{\tau'/x\} \cup F$ and we conclude by observing that $\sigma'\{\tau'/x\} \equiv \alpha.\sigma'_1\{\tau'/x\}$.

($\sigma \equiv \sigma_1 + \sigma_2$). We have $\sigma' \equiv \sigma'_1 + \sigma'_2$ and $E = E_1 \cup E_2$, where $E(\sigma_1) = \sigma'_1 : E_1$ and $E(\sigma_2) = \sigma'_2 : E_2$. We examine only one interesting case, when $x \in \mathrm{fv}(\sigma_1) \setminus \mathrm{fv}(\sigma_2)$. By induction hypothesis we derive $E(\sigma_1\{\tau/x\}) = \sigma'_1\{\tau'/x\} : E_1\{\tau'/x\} \cup F$. Now $E(\sigma\{\tau/x\}) = E(\sigma_1\{\tau/x\} + \sigma_2) = \sigma'_1\{\tau'/x\} + \sigma'_2 : E_1\{\tau'/x\} \cup E_2 \cup F$ and we conclude by observing that $\sigma'\{\tau'/x\} \equiv \sigma'_1\{\tau'/x\} + \sigma'_2$ and $E\{\tau'/x\} = E_1\{\tau'/x\} \cup E_2$.

($\sigma \equiv \sigma_1 \oplus \sigma_2$). Similar to the previous case.

($\sigma \equiv \mathrm{rec}\, x = \sigma_1$). Trivial since $x \not\in \mathrm{fv}(\sigma)$.

($\sigma \equiv \mathrm{rec}\, y = \sigma_1$, $y \neq x$). If $x \in \mathrm{fv}(\sigma)$, then $x \in \mathrm{fv}(\sigma_1)$ because $x \neq y$. We distinguish two subcases. Assume $y \not\in \mathrm{fv}(\sigma_1)$. Then $E(\sigma) = E(\sigma_1) = \sigma' : E$. By induction hypothesis we derive $E(\sigma_1\{\tau/x\}) = \sigma'\{\tau'/x\} : E\{\tau'/x\} \cup F$. From $\mathrm{bv}(\sigma) \cap \mathrm{fv}(\tau) = \emptyset$ we obtain $y \not\in \mathrm{fv}(\tau)$, hence we conclude $E(\sigma\{\tau/x\}) = E(\mathrm{rec}\, y = \sigma_1\{\tau/x\}) = \sigma'\{\tau'/x\} : E\{\tau'/x\} \cup F$. Assume $y \in \mathrm{fv}(\sigma_1)$. Then $\sigma' \equiv y$ and $E = E' \cup \{y = \sigma'_1\}$ where $E(\sigma_1) = \sigma'_1 : E'$. By induction hypothesis we derive $E(\sigma_1\{\tau/x\}) = \sigma'_1\{\tau'/x\} : E'\{\tau'/x\} \cup F$. Now $E(\sigma\{\tau/x\}) = E(\mathrm{rec}\, y = \sigma_1\{\tau/x\}) = y : E'\{\tau'/x\} \cup F \cup \{y = \sigma'_1\{\tau'/x\}\}$ and we conclude by observing that $\sigma'\{\tau'/x\} \equiv y$ and $E\{\tau'/x\} = E'\{\tau'/x\} \cup \{y = \sigma'_1\{\tau'/x\}\}$. □

Now that we have defined the semantics of a recursive contract in terms of unfolded contracts, we can extend to recursive contracts all the definitions introduced for recursive contracts. For example, if σ is a recursive contract, then $\sigma \Downarrow \mathbf{r}$ if and only if $[\sigma] \Downarrow \mathbf{r}$.

By Theorem 4.2.1 of [Courcelle 1983] we also know that the syntax of recursive contracts is complete with respect to the set of unfolded contracts. In particular, every unfolded contract is a component of the unique solution of some regular system. A regular system is nothing but a flattened recursive contract, in which every recursion has been turned into an equation.

The second syntax we consider is reminiscent of regular expressions, with the remarkable difference that we have two different sum operators $+$ and $\oplus$ for external and internal choice, respectively. Correspondingly we also have two different Kleene star operators $*$ and $^{@}$. This yields to the definition of *regular* contracts and filters as the finite terms inductively generated by the following grammars

$$\begin{array}{rcl} \sigma & ::= & \mathbf{0} \mid \alpha \mid \sigma;\sigma \mid \sigma + \sigma \mid \sigma \oplus \sigma \mid \sigma^* \mid \sigma^{@} \\ \boldsymbol{f} & ::= & \mathbf{0} \mid \alpha \mid \boldsymbol{f};\boldsymbol{f} \mid \boldsymbol{f} \vee \boldsymbol{f} \mid \boldsymbol{f} \wedge \boldsymbol{f} \mid \boldsymbol{f}^* \end{array}$$

The semantics of a regular contract τ can be indirectly given by translating it into a recursive contract. The main issue of this translation is handling sequential composition, which must be reduced to action prefixes. We parameterize the translation with a *continuation* on which we accumulate actions while scanning

the regular contract from right to left. We write $[\tau]_\sigma$ for the recursive contract resulting from the encoding of the regular contract τ, when the continuation is the recursive contract σ. We must ensure that the translation does not yield degenerate recursive contracts in which some bound variable occurs unguarded, since such terms do not have a proper semantics. To this purpose we inductively define a guardedness predicate $\mathrm{G}(\sigma)$ guaranteeing that in the recursive contract $[\sigma]_x$ the variable x always occurs under a prefix. The $\mathrm{G}(\sigma)$ predicate is inductively defined as follows:

—$\mathrm{G}(\mathbf{0})$ and $\mathrm{G}(\alpha)$;

—if $\mathrm{G}(\sigma)$ or $\mathrm{G}(\tau)$, then $\mathrm{G}(\sigma;\tau)$;

—if $\mathrm{G}(\sigma)$ and $\mathrm{G}(\tau)$, then $\mathrm{G}(\sigma + \tau)$ and $\mathrm{G}(\sigma \oplus \tau)$.

and $[\tau]_\sigma$ is inductively defined thus:

$$
\begin{aligned}
[\mathbf{0}]_\sigma &= \mathbf{0} \\
[\alpha]_\sigma &= \alpha.\sigma \\
[\tau\,;\tau']_\sigma &= [\tau]_{[\tau']_\sigma} \\
[\tau + \tau']_\sigma &= [\tau]_\sigma + [\tau']_\sigma \\
[\tau \oplus \tau']_\sigma &= [\tau]_\sigma \oplus [\tau']_\sigma \\
\llcorner\tau^*\lrcorner_\sigma &= \mathrm{rec}\, x = \sigma + [\tau]_x \quad (x \text{ fresh and } \mathrm{G}(\tau)) \\
\llcorner\tau^@\lrcorner_\sigma &= \mathrm{rec}\, x = \sigma \oplus \llcorner\tau\lrcorner_x \quad (x \text{ fresh and } \mathrm{G}(\tau))
\end{aligned}
$$

We write $\llcorner\tau\lrcorner$ for $\llcorner\tau\lrcorner_{\mathbf{0}}$. Note that neither $\llcorner\tau^*\lrcorner_\sigma$ nor $\llcorner\tau^@\lrcorner_\sigma$ are defined if x occurs unguarded in $[\tau]_x$. Similarly to what happens to the external choice operator $+$, the external Kleene star may hide an internal Kleene star if the contract being iterated shares an action with the continuation. For instance,

$$\llcorner\alpha^*\lrcorner_\alpha = \mathrm{rec}\, x = \alpha + \alpha.x \;::\; \mathrm{rec}\, x = \alpha \oplus \alpha.x = \llcorner\alpha^@\lrcorner_\alpha$$

It is well known that (nondeterministic) regular expressions are not complete with respect to nondeterministic finite state automata. In our context this means that there are recursive contracts that cannot be generated by any regular contract. For instance, there is no regular contract whose translation is the recursive contract $\mathrm{rec}\, x = (a.x + b) \oplus (c.x + d)$. Roughly speaking, the reason lies in the fact that the same recursion variable x is shared among two different "loops" in the recursive contract. Characterizations of recursive contracts admitting equivalent regular contracts can be found in [De Nicola and Labella 2003; Baeten et al. 2007].

5.2 Encoding wscl activity diagrams

A wscl activity diagram [Banerji et al. 2002] is a tuple $(Q, \mathrm{a}, \delta, x_1, x_n)$ where $Q = \{x_1, \ldots, x_n\}$ is a finite set of *interactions*, $\mathrm{a} = \{\alpha_1, \ldots, \alpha_m\}$ is a finite set of actions representing ingoing and outgoing *document types*, $\delta \subseteq Q \times \mathrm{a} \times Q$ is the *transition relation*, $x_1 \in Q$ is the *initial interaction* and $x_n \in Q$ is the *final interaction*. We write $x \xrightarrow{\alpha} y$ if $(x, \alpha, y) \in \delta$; we write $x \xrightarrow{\alpha}$ if there exists $y \in Q$ such that $x \xrightarrow{\alpha} y$; we write $x \not\xrightarrow{\alpha}$ if not $x \xrightarrow{\alpha}$.

According to the wscl specification, the following well-formedness conditions must hold:

(1) every interaction must be reachable from x_1, namely for every $y \in Q$ and $y \neq x_1$ there exist $\alpha_1, \ldots, \alpha_k$ such that $x_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_k} y$;
(2) for every $x \in Q$, if there exist $a \in \mathrm{a}$ such that $x \xrightarrow{a}$, then for every $\bar{b} \in \mathrm{a}$ we have that $x \xrightarrow{\bar{b}}$;
(3) x_n must not have any outgoing transition, that is $x_n \not\xrightarrow{\alpha}$ for every $\alpha \in \mathrm{a}$.

The encoding of an interaction x in a wscl activity diagram when the interactions Q have not been encoded yet is denoted by $E(x, Q)$ and is defined as follows:

$$E(x, Q) \stackrel{\text{def}}{=} \begin{cases} x & \text{if } x \neq 0 \\ \mathrm{rec}\, x = \bigoplus_{a \in \mathrm{a}, \delta(x,a) \neq \emptyset} \bigoplus_{y \in \delta(x,a)} \bar{a}.E(y, Q \setminus \{x\}) & \\ & \text{if } x \in Q \text{ and } x \xrightarrow{\bar{a}} \text{ for some } \bar{a} \in \mathrm{a} \\ \mathrm{rec}\, x = \sum_{a \in \mathrm{a}, \delta(x,a) \neq \emptyset} \sum_{y \in \delta(x,a)} a.E(y, Q \setminus \{x\}) & \text{otherwise} \end{cases}$$

Because of well-formedness condition (1), the whole activity diagram is encoded; because of well-formedness condition (2), the last two cases in the definition of $E(x, Q)$ are mutually exclusive; because of well-formedness condition (3), we have $E(x_n, Q) \simeq \mathbf{0}$. The encoding of a wscl activity diagram is now defined as $E(x_1, Q)$.

5.3 Typing ws-bpel activities

ws-bpel [Alves et al. 2007] is an Oasis standard language for the description of business processes. It builds on top of standard Web service technologies, such as wsdl, for providing a detailed, structured description of Web services behavior, including exception and compensation handlers. Being a concrete Web service specification language, ws-bpel is hard to formalize thoroughly. In our setting, however, we are merely concerned with the observable behavior of a Web service, hence we can disregard any detail that is not directly related with the interactions of the Web service with the external world. Furthermore, we gain in clarity by getting rid of the heavyweight xml syntax used in ws-bpel and by preferring a streamlined algebraic presentation, which the reader will easily match with the original language.

$$\begin{array}{lll} A ::= & \mathrm{action}(\alpha) & \\ \mid & \mathrm{pick}(a_1.A_1, \ldots, a_n.A_n) & n \geq 0 \\ \mid & \mathrm{sequence}(A_1, \ldots, A_n) & n \geq 0 \\ \mid & \mathbf{if}(A_1, \ldots, A_n) & n \geq 1 \\ \mid & \mathrm{flow}(A_1, \ldots, A_n) & n \geq 0 \\ \mid & \mathrm{while}(A) & \end{array}$$

The above grammar describes ws-bpel so-called *activities* (i.e., processes). The activity $\mathrm{action}(\bar{a})$ denotes the invocation of operation a or, more generally, the act of sending a message on a channel identified by a; it can be used for representing both invoke and reply activities in ws-bpel. The activity $\mathrm{action}(a)$ denotes the act of waiting for an interaction on a channel identified by a; it can be used for representing receive activities. The pick activity allows the service to provide multiple operations, among which the client can choose which one to execute. Each action a_i denotes an operation that, when invoked, causes the corresponding activity

Table IV. Type system for ws-bpel activities.

$$\text{(action)}\ \ \text{action}(\alpha) : \alpha \qquad \text{(pick)}\ \ \frac{A_1 : \sigma_1 \quad \cdots \quad A_n : \sigma_n}{\text{pick}(a_1.A_1, \ldots, a_n.A_n) : a_1;\sigma_1 + \cdots + a_n;\sigma_n}$$

$$\text{(sequence)}\ \ \frac{A_1 : \sigma_1 \quad \cdots \quad A_n : \sigma_n}{\text{sequence}(A_1, \ldots, A_n) : \sigma_1;\ldots;\sigma_n} \qquad \text{(if)}\ \ \frac{A_1 : \sigma_1 \quad \cdots \quad A_n : \sigma_n}{\mathbf{if}(A_1, \ldots, A_n) : \sigma_1 \oplus \cdots \oplus \sigma_n}$$

$$\text{(flow)}\ \ \frac{A_1 : \sigma_1 \quad \cdots \quad A_n : \sigma_n \quad \text{actions}(\sigma_i) \cap \text{co}(\text{actions}(\sigma_j)) = \emptyset^{\,i,j \in 1..n}}{\text{flow}(A_1, \ldots, A_n) : \sigma_1 \quad \cdots \quad \sigma_n} \qquad \text{(while)}\ \ \frac{A : \sigma}{\text{while}(A) : \sigma^{\circledR}}$$

A_i to be executed; the sequence activity sequentially activates the specified sub-activities, A_{i+1} starting only when A_i is completed; the **if** activity performs an internal choice among the specified sub-activities according to the result of some Boolean conditions that we leave unspecified in the syntax; the while activity sequentially executes the specified sub-activity as long as some Boolean condition (once more left unspecified) is verified; the flow denotes the parallel composition of the specified sub-activities; it completes when all the sub-activities have completed. We write empty for sequence*()*, for pick*()*, and for flow*()*.

Table IV shows the type system for ws-bpel activities, where a judgment $t\text{-}A : \sigma$ associates an activity A with its contract σ. Most rules are completely straightforward as ws-bpel activities map very naturally to the contract operators described in §5.1. The only rules that deserve some explanation are **(flow)** and **(while)**. Regarding **(while)**, the choice as to whether the sub-activity A must be executed once more or the repetition has ended is made internally, by evaluating some unspecified condition. Hence the use of the internal Kleene star ® in the resulting contract. Because of the side-condition in the semantics of $\sigma^{@}$, not every while activity is well typed. For instance, while*(***if***(*empty*,* action*(*a*)))* is not well typed because the contract of the repeated activity has an empty ready set. Regarding **(flow)**, the sub-activities are allowed to run concurrently and independently of each other. Thus, the contract of a flow activity is given by all the possible interleaving of actions in the contracts of the sub-activities. This interleaving is computed by the operator, which is defined as follows:

$$\sigma \ \tau \stackrel{\text{def}}{=} \text{EB}_{\sigma \Downarrow \mathbf{r}, \tau \Downarrow \mathbf{s}}\Big(\bigsqcup_{\alpha \in \mathbf{r}} \alpha;(\sigma(\alpha) \ \ \tau) + \bigsqcup_{\beta \in \mathbf{s}} \beta;(\sigma \ \ \tau(\beta))\Big)$$

It is easy to verify that $\sigma \ \tau$ is well defined (it is a regular contract) and that is a commutative, associative operator whose neutral element is **0**. The premise $\text{actions}(\sigma_i) \cap \text{co}(\text{actions}(\sigma_j)) = \emptyset$ (we use $\text{actions}(\sigma)$ to denote the set of all actions occurring in σ) imposes that no message exchange is allowed within the same ws-bpel business process.[4] This allows us to express as a simplified form of the *expansion law* as it is found, for instance, in [Hennessy 1988].

[4] In ws-bpel, actions used for synchronizing activities of a flow must be invisible outside the flow.

We do not define any operational semantics for the activities. As a matter of fact this is already given by the type systems of Table IV: contracts being behavioral types, they faithfully describe the operational semantics of activities. More importantly, our theory of contracts provides us with a formal tool for reasoning about safe replacement and upgrade of ws-bpel activities, by comparing the corresponding contracts. For instance, the depth and width subtyping properties enjoyed by $\leq$ tell us that it is safe to replace an activity A with an activity sequence(A, A') and also that it is safe to replace $\mathsf{pick}(\alpha_1.A_1, \ldots, \alpha_m.A_m)$ with $\mathsf{pick}(\alpha_1.A_1, \ldots, \alpha_n.A_n)$ where $n \geq m$. In the first case, we are appending additional functionalities to some business process; in the second case, we are providing additional alternative functionalities to a business process.

The following result shows that we can also derive interesting substitution properties for sequence and flow:

Proposition 5.2. *Let* $\mathrm{actions}(\sigma) \cap \mathrm{actions}(\tau) = \emptyset$. *Then* $\sigma;\tau \leq \sigma \parallel \tau$.

Proof. It is sufficient to prove that $W \stackrel{\text{def}}{=} \{(\sigma, \sigma \parallel \tau) \mid \mathrm{actions}(\sigma) \cap \mathrm{actions}(\tau) = \emptyset\} \cup \{(\sigma;\tau, \sigma \parallel \tau) \mid \mathrm{actions}(\sigma) \cap \mathrm{actions}(\tau) = \emptyset\}$ is a weak subcontract relation. Let $(\sigma, \sigma \parallel \tau) \in W$ and assume $\sigma \parallel \tau \Downarrow \mathbf{r}$. By definition of $\sigma \parallel \tau$ there exist $\mathbf{r}'$ and s such that $\sigma \Downarrow \mathbf{r}'$ and $\tau \Downarrow$ s and $\mathbf{r} = \mathbf{r}' \cup$ s, from which we derive $\mathbf{r}' \subseteq \mathbf{r}$. Let $\alpha \in \mathbf{r}'$. Then $(\sigma \parallel \tau)(\alpha) \equiv \sigma(\alpha) \parallel \tau$ by definition of $\sigma \parallel \tau$ and we conclude $(\sigma(\alpha), \sigma(\alpha) \parallel \tau) \in W$ by definition of W. Let $(\sigma;\tau, \sigma \parallel \tau) \in W$ and assume $\sigma \parallel \tau \Downarrow \mathbf{r}$. Then there exist $\mathbf{r}'$ and s such that $\sigma \Downarrow \mathbf{r}'$ and $\tau \Downarrow$ s and $\mathbf{r} = \mathbf{r}' \cup$ s. We have two cases: (1) if $\mathbf{r}' \neq \emptyset$, then $\sigma;\tau \Downarrow \mathbf{r}'$ and we derive $\mathbf{r}' \subseteq \mathbf{r}$; (2) if $\mathbf{r}' = \emptyset$, then $\sigma;\tau \Downarrow$ s and we derive s $\subseteq \mathbf{r}$. In case (1), assume $\alpha \in \mathbf{r}'$. From the encoding of $\sigma;\tau$ and from the hypothesis $\mathrm{actions}(\sigma) \cap \mathrm{actions}(\tau) = \emptyset$ we have $(\sigma;\tau)(\alpha) \equiv \sigma(\alpha);\tau$ and by definition of $\parallel$ we have $(\sigma \parallel \tau)(\alpha) \equiv \sigma(\alpha) \parallel \tau$ and we conclude $(\sigma(\alpha);\tau, \sigma(\alpha) \parallel \tau) \in W$ by definition of W. In case (2), assume $\alpha \in$ s. From the encoding of $\sigma;\tau$ and from the hypothesis $\mathrm{actions}(\sigma) \cap \mathrm{actions}(\tau) = \emptyset$ we obtain $(\sigma;\tau)(\alpha) \equiv \tau(\alpha)$ and by definition of $\parallel$ we have $(\sigma \parallel \tau)(\alpha) \equiv \sigma \parallel \tau(\alpha)$ so we conclude $(\tau(\alpha), \sigma \parallel \tau(\alpha)) \in W$ again by definition of W. □

As a corollary of Proposition 5.2 observe that $\sigma \leq \sigma \parallel \tau$ when σ and τ share no common action. Let $\boldsymbol{f} : \sigma;\tau \leq \sigma \parallel \tau$ and let $t\text{-}A : \sigma$ and $t\text{-}B : \tau$. Proposition 5.2 can be interpreted in two different ways: when reading $\sigma;\tau \leq \sigma \parallel \tau$ from left to right, the proposition gives us sufficient conditions by which we can replace sequence(A, B) with $\mathsf{flow}(A, B)$ when A and B are independent activities and we want to increase the service throughput by taking advantage of parallelism (for instance, because the machine hosting the Web service has been upgraded and is now multiprocessor). In this case the clients of the old, sequential Web service can still interact successfully with the upgraded, parallel one, provided that the interaction is shielded by $\boldsymbol{f}$.

On the other hand, when reading $\sigma;\tau \leq \sigma \parallel \tau$ from right to left, the proposition gives us sufficient conditions by which we can approximate the behavior of $\mathsf{flow}(A, B)$ with that of sequence(A, B). Indeed, the size of contract $\sigma \parallel \tau$ may grow exponentially with respect to the size of σ and τ because of the use of continuations $\sigma(\alpha)$ and $\tau(\alpha)$ and of the interleaving semantics in the definition of $\parallel$. For instance, we have

$$a.\bar{b} \parallel c.\bar{d} = a.(\bar{b}.c.\bar{d} + c.(\bar{b}.\bar{d} + \bar{d}.\bar{b})) + c.(a.(\bar{b}.\bar{d} + \bar{d}.\bar{b}) + \bar{d}.a.\bar{b})$$

and it might be desirable to approximate $a.\bar{b} \;\&\; c.\bar{d}$ with $a.c.\bar{b}.\bar{d} + a.c.\bar{d}.\bar{b}$. However, doing so without filters can be dangerous, as the following example shows. Consider the client contract $\rho \stackrel{\text{def}}{=} \bar{a}.(b.b.0 + \bar{c}.b.d.0)$. Then $\rho \simeq a.c.\bar{b}.\bar{d}$, hence a client having contract ρ would be declared compliant with the service whose approximate contract is $a.c.\bar{b}.\bar{d} + a.c.\bar{d}.\bar{b}$. However, by inspecting the expansion of $a.\bar{b} \;\&\; c.\bar{d}$ we realize that the behavior of the service does actually account for a $\bar{b}$ action right after the action a, so the client (process) might get stuck trying to read a second b after the first one. By applying the filter $a.c.\bar{b}.\bar{d} + a.c.\bar{d}.\bar{b}$, we prevent any synchronization on b to happen during the second interaction, thus guaranteeing that the client successfully terminates.

5.4 On implementing filters

We have presented filters as behavioral coercions that enlarge the set of Web services a client is compliant with. Basically, the filter mediates the interaction between client and service by forbidding actions that can potentially lead the client to a deadlock. The filter, however, has no power over the internal choices made independently by client and service. In our theory, this latter fact is remarkably rendered by rules (IChoice) and (EChoice) (see Table I on page 22), in which the *same* filter must be applicable for all the branches of internal and external choices, in order to work correctly. Do filters actually play a role in real-world Web services? If so, do they admit effective, and hopefully efficient, implementations? As regards the first question, we notice that a filter is actually a well known actor in the Web service scenario: it is an example of Web service *orchestrator*. An orchestrator is simply a process whose task is to coordinate other processes in such a way so as to guarantee that their interaction eventually leads to the achievement of a goal (in our setting, the goal being client satisfaction).

As regards the implementation of filters, we discuss it in the rest of the section.

5.4.1 *Implementing filters as join patterns.* A first observation is that filters can be rendered by means of *binary join patterns* (in the style of the Join calculus [Fournet and Gonthier 1996; Fournet et al. 1996]) of the form $\alpha \;\&\; \beta$, which can be thought of as an atomic action that can be executed provided that $\bar{\alpha}$ and $\bar{\beta}$ are simultaneously available in the execution environment. Then, a filter φ may be implemented as a (finite-state) process $C[\![\varphi]\!]$ as follows

$$C[\![\varphi]\!] = \sum_{\varphi \xrightarrow{\alpha} \varphi'} \alpha \;\&\; \bar{\alpha'}.C[\![\varphi']\!]$$

where we use α' to distinguish the action α performed by the filtered service, so that it is not confused with the action α as it is seen by the client. Then a client P and a service Q safely interact with each other under the supervision of the filter/orchestrator:

$$P \;\|\; C[\![\varphi]\!] \;\|\; Q\{\alpha'_1/\alpha_1, \ldots, \alpha'_n/\alpha_n\}$$

where $\alpha_1, \ldots, \alpha_n$ are the actions occurring in Q and $\|$ denotes the usual parallel composition of processes.

The problem then reduces to the effective implementation of join patterns. It is well known that implementations of the Join calculus all pose strong requirements over the channels being joined together, namely that they must all be created simultaneously with the patterns in which they are involved, and that they must all

be local to the host that created them. However, it has also been shown in [Laneve and Padovani 2006] how to partly relax these constraints so that only locality is actually required in order to avoid a global consensus problem, and that join patterns can be dynamically attached to the site hosting the channels being joined.

5.4.2 *Filters as one-position buffers.* The second observation is that, for an interesting subclass of processes, join patterns are not necessary at all. If we assume that, at any time, the service can only (internally) decide to send messages, or can only (externally) wait for messages, then the compilation scheme sketched above reduces to the straightforward process

$$\mathrm{C}[f] = \sum_{f \xrightarrow{a} f'} a.\overline{a'}.\mathrm{C}[f'] + \sum_{f \xrightarrow{\overline{a}} f'} a'.\overline{a}.\mathrm{C}[f']$$

in which, for every f, at most one of the two sums is nonempty. This subclass is interesting because it exactly characterizes processes behaving according to *session types* [Honda 1993; Takeuchi et al. 1994; Honda et al. 1998], in which at any time only one process, either the client or the service, decides the next action to be executed. In this respect, the generality of our contract language may at first appear excessive, since it allows a mixture of input and output actions irrespective of the choice operators with which they are combined. In particular, it seems natural to restrict output actions to internal choices, and input actions to external choices. However, it is clear from Table IV and from the definition of the operator given earlier that input and output actions can occur as guards in both internal and external choices of real world Web services contracts.

5.4.3 *Implementing filters in* ws-bpel. The language of filters we have adopted is very simple. Given $f : \sigma \leq \tau$, the structure of f tells us very little about the actual behavior of σ and τ. It is reasonable to expect that, by enriching the language of filters with constructs that more faithfully describe the structure of the *proof* that relates σ and τ, one is able to provide efficient implementations in a wider range of situations. Nevertheless even if we want to implement just these "simple" filters by means of ws-bpel processes, we cannot hope to obtain much more than what we did with one-position buffers. The point of the encoding in §5.4.1 is to exploit join patterns for detecting the simultaneous presence, on the server and on its client, of an action and its coaction. This cannot be expressed (at least not straightforwardly) in a ccs-like formalism nor in ws-bpel, which solely relies on low-level communication primitives. Consequently we must restrict our attempt of encoding filters as ws-bpel processes to staged computations in which just one of the partners has the floor. This, combined with the fact that the syntax of pick forces external choices to be performed on inputs, yields to a subcontracting hierarchy very close to the one relating session types [Gay and Hole 2005].

In what follows we outline a formalization of this hierarchy and its benefits in ws-bpel. The point is not to study the expressivity of ws-bpel but to show that the theory presented in this paper can be applied to ws-bpel and to ws-bpel processes in the current form. In a nutshell, if we want to check whether two ws-bpel processes are or can be made compliant, then what we have to do is (*i*) to extract their contracts by means of the type system in Table IV, (*ii*) to check whether the extracted contracts are compatible with a staged computation (see

Definition 5.3 below), and (*iii*) to automatically synthesize the ws-bpel process implementing the filter that makes the client compliant with the service. Thus the theory is immediately applicable to existing ws-bpel processes to combine them more flexibly (thanks to the width subtyping that allows us to update services with new features) without the need of adding new primitives or constructors (such as session types labels and labeled selections) to ws-bpel nor of modifying the code of existing processes.

More precisely, the filters that we can reasonably encode in ws-bpel are those that never filter out output messages and that relate staged contracts, having the following form.

Definition 5.3 (staged contract). *We say that the (service) contract σ is* staged *if either (1) $\sigma \simeq \bigoplus_{i\in I} a_i;\sigma_i$ and for every $i, j \in I$ such that $i \neq j$ we have $a_i \neq a_j$ and each σ_i is staged or (2) $\sigma \simeq \bigoplus_{i\in I} (a_{i1} \cdots a_{in_i});\sigma_i$ and for every $i, j \in I$ such that $i \neq j$ we have $a_{i1} \neq a_{j1}$ and each σ_i is staged.*

In case (1) we say that σ is staged if it describes a service that lets the client decide which message to send. In case (2) we say that σ is staged if it describes a service that can be in one of $|I|$ different states and in each state $i \in I$ the service sends a message a_{i1} that distinguishes that state from all the others, along with possibly more messages $a_{i2}, \ldots, a_{in_i}$ (observe that $|I| > 1$ implies $n_i > 0$ for every $i \in I$). Then, the service continues behaving as a staged contract σ_i.

A filter that never filters out output messages is called *input filter* and is formally defined below.

Definition 5.4 (input filter). *We say that f is an* input filter *for the (service) contract σ if $\sigma \xrightarrow{\phi\bar{a}}$ and $f \xrightarrow{\phi} f'$ implies $f' \xrightarrow{\bar{a}}$.*

Namely, an input filter never filters out any output action, unless this is guarded by an input action that has been filtered out. Given an input filter f for a staged (service) contract σ, the ws-bpel process that implements f, denoted by $F(f, \sigma)$, can be defined as follows:

$$F(f,\sigma) \stackrel{\text{def}}{=} \begin{cases} \text{pick}(a_i.\text{action}(\bar{a}^I_i); F(f(a_i), \sigma_i), \ldots)^{(i\in I, f\xrightarrow{a_i})} & \text{if } \sigma \simeq \bigoplus_{i\in I} a_i.\sigma_i \\ \text{pick}(a^I_{i1}.\text{sequence}(\text{action}(a^I_{i2}), \ldots, \text{action}(a^I_{in_i}), & \\ \qquad \text{flow}(\text{action}(\bar{a}_{i1}), \ldots, \text{action}(\bar{a}_{in_i})), & \\ \qquad F(f(\bar{a}_{i1}\cdots\bar{a}_{in_i}), \sigma_i)), \ldots)^{(i\in I)} & \\ \qquad\qquad \text{if } \sigma \simeq \bigoplus_{i\in I} (\bar{a}_{i1} \cdots \bar{a}_{in_i});\sigma_i \end{cases}$$

If σ is an external choice of input actions, then the filter simply waits for a message on one of those input actions a_i that have not been filtered out ($f \xrightarrow{a_i}$). Once such a message is received, the filter delivers it to the service. If σ is an internal choice of (possibly concurrent) output actions, then the filter waits for a message a_{i1} from the service. Since σ is staged, all the a_{i1}'s are distinct hence the pick activity is well formed. When a message is received, the filter unambiguously knows the state the service is in, hence it collects all the other messages produced by the service in that state. Then, all the collected messages are delivered to the

client, because f is an input filter.

6. CONCLUSION AND FUTURE WORK

This paper provides a foundation for behavioral typing of Web services and it promotes service reuse and/or redefinition by the introduction of a subcontract relation.

Our approach reconciles two hitherto apparently incompatible requirements. On the one hand a subcontract relation must allow a service to be replaced or upgraded by offering more operations (width subtyping), longer interaction patterns (depth subtyping) and/or more deterministic ones. On the other hand this must be done without disrupting the behavior of clients.

Filters provide the technical device that makes it possible. Although we initially defined filters essentially as technical mechanism to couple clients and services, filters turn out to have an elegant logical justification: they are explicit coercions between related contracts. Following the Curry-Howard isomorphism filters can be interpreted as proofs of a sound and complete deduction system for the subcontract relation. Such deduction system simultaneously refines and extends Hennessy's classical axiomatization of the must testing preorder. Its algorithmic counterpart is obtained as a cut elimination process, which proves the coherence of subcontracting as a logical system. The canonical proof, the one produced by the algorithmic deduction system, is characterized in terms of an order relation on filters, and the algorithmic presentation allows us to show the decidability both of the subcontracting relation and of filter inference.

The theory of subcontracting is independent of the language used to implement services and clients. We do not rely on a particular language nor on a particular paradigm (objects, process algebras, functions, ...). By defining some minimal requirements on the language (in a nut-shell, the observable behavior of its programs must be faithfully captured by contracts), we establish the soundness of our contract system: clients always terminate interactions with any, possibly filtered, compliant service. We have also shown that we do not need either to extend ws-bpel syntax or to reprogram existing ws-bpel processes in order to apply to them the theory presented in this paper and thus reuse them in more contexts.

Filters thus play the double role of a proof tool and of programming glue between clients and services. As an aside it is nice to notice that filters can encode ccs and π-calculus restrictions: $(\nu a)P = \varphi_{aP}[P]$ where

$$\varphi_{aP} = \bigvee_{\alpha \in (\mathrm{fn}(P) \cup \mathrm{co}(\mathrm{fn}(P))\setminus\{a,\bar{a}\}} \alpha.\varphi_{aP} \ .$$

That is, a restriction is nothing but a recursive filter that allows all actions apart from the restricted one.

Even if in this presentation we applied filters to services, in practice it is the client's responsibility to apply them. A client searching for a service with a given contract will receive as answer to its query the reference of a service together with a filter that allows the client to use the service. Thus the filter must be computed by the query engine, which is why the algorithmic inference of filters is crucial for a practical application.

Actually, it is more realistic to imagine that a query will be answered with several different contracts requiring filters that may be unrelated to each other. Therefore a second use of filters could be that of refining the search space, by specify-

ing in a query a minimum acceptable filter. In this way the client could specify which of the possible behaviors of its "canonical" service are considered mandatory and not to be filtered out. For instance, when searching for services implementing the behavior described in Figure 1 we could specify, along with the query, the filter $\mathsf{Login.\overline{ValidLogin}.Query.\overline{Catalog}.AddToCart.\,Buy.(CreditCard.\overline{Valid} \vee BankTransfer.\overline{Valid})}$ thus obtaining only services that may complete a sale, avoiding useless services such as those with contract $\mathsf{Login.\overline{InvalidLogin}}$.

Several future research directions stem from this work. The following is a non-exhaustive list:

—*Higher-order contracts:* In the current formalism synchronization does not carry any information. Thus a natural next step is the introduction of higher order channels *à la* π-calculus.

—*Asymmetric choices:* The choice operators are commutative. We could try to relax this property in order to give the summands different priorities, which is impossible with the current definitions. For instance, there is no way for a client that has to use a service with contract $(a + b) \oplus a$ to specify that it wants to connect with b if this action is available, and with a otherwise (in order to be compliant it must accept a possible synchronization with a). It is unclear to which extent such constructs would affect the $\dashv$ preorder over contracts.

—*Contract morphisms:* The only morphisms between contracts we have considered are filters. Since filters are coercions, then by definition they essentially do not alter the semantics of objects. One could try to consider more expressive morphisms (e.g. renaming or reordering of actions) and to perform service discovery modulo such morphisms: when searching for services of a given contract a client could be returned a service and a conversion function that adapts the interaction pattern of the client to the service at issue (somewhat similar to, but less stringent than, libraries searches modulo type isomorphisms [Rittri 1993; Di Cosmo 1995]). This could set the basis of a new theory of orchestration where light and highly distributed orchestrators would be implemented by filters and contract morphisms.

This could later be extended to richer query/discovery languages obtained by adding union, intersection and negation types on the basis of the set-theoretic interpretation presented here and of the work on semantic subtyping [Castagna and Frisch 2005].

—*Relation with other formalisms:* Finally, connection with other formalisms such as linear logic, session types, and game semantics must surely be deeply investigated. In particular, as regards the semantic aspects, it is interesting to notice that clients and services introduce a notion of orthogonality which suggests that a realizability semantics for contracts is worth exploring.

REFERENCES

Alves, A., Arkin, A., Askary, S., Barreto, C., et al. 2007. *Web Services Business Process Execution Language Version 2.0*. OASIS Standard, http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html.

Baeten, J. C. M., Corradini, F., and Grabmayer, C. A. 2007. A characterization of regular expressions under bisimulation. *J. ACM 54,* 2, 6.

Banerji, A., Bartolini, C., Beringer, D., Chopella, V., et al. 2002. *Web Services Conversation Language (*wscl*) 1.0*. W3C Note, http://www.w3.org/TR/2002/NOTE-wscl10-20020314.

Bellwood, T., Capell, S., Clement, L., Colgrave, J., et al. 2005. uddi *Version 3.0.2*. OASIS Standard, http://uddi.org/pubs/uddi-v3.0.2-20041019.htm.

Bravetti, M. and Zavattaro, G. 2007. Towards a unifying theory for choreography conformance and contract compliance. In *Proc. of the 6th Intl. Symposium on Software Composition*. Springer.

Brinksma, E., Scollo, G., and Steenbergen, C. 1995. Lotos specifications, their implementations and their tests. 468–479.

Bruce, K. and Longo, G. 1990. A modest model of records, inheritance and bounded quantification. *Information and Computation 87,* 1/2, 196–240.

Carbone, M., Honda, K., and Yoshida, N. 2007a. A calculus of global interaction based on session types. *Electronic Notes in Theoretical Computer Science 171,* 3, 127–151.

Carbone, M., Honda, K., and Yoshida, N. 2007b. Structured communication-centred programming for web services. In *ESOP '07, 16th European Symposium on Programming*. LNCS 4421. Springer.

Cardelli, L. 1988. A semantics of multiple inheritance. *Information and Computation 76*, 138–164.

Carpineti, S., Castagna, G., Laneve, C., and Padovani, L. 2006. A formal account of contracts for Web Services. In *3rd Int. Workshop on Web Services and Formal Methods*. LNCS 4184. Springer.

Castagna, G. and Frisch, A. 2005. A gentle introduction to semantic subtyping. In *PPDP '05* ACM Press (full version) and *ICALP '05,* LNCS 3580, Springer (summary) (July). Joint ICALP-PPDP keynote talk.

Castagna, G., Gesbert, N., and Padovani, L. 2007. A theory of contracts for web services. In *PLAN-X '07, 5th ACM-SIGPLAN Workshop on Programming Language Technologies for XML*.

Castagna, G., Gesbert, N., and Padovani, L. 2008. A theory of contracts for web services. In *POPL '08, 35th ACM Symposium on Principles of Programming Languages*. 261–272.

Chen, G. 2004. Soundness of coercion in the calculus of constructions. *Journal of Logic and Computation 14,* 3, 405–427.

Chinnici, R., Haas, H., Lewis, A.-A., Moreau, J.-J., et al. 2007. *Web Services Description Language (*wsdl*) Version 2.0 Part 2: Adjuncts*. W3C Recommendation, http://www.w3.org/TR/wsdl20-adjuncts/.

Chinnici, R., Moreau, J.-J., Ryman, A., and Weerawarana, S. 2007. *Web Services Description Language (*wsdl*) Version 2.0 Part 1: Core Language*. W3C Recommendation, http://www.w3.org/TR/wsdl20/.

Courcelle, B. 1983. Fundamental properties of infinite trees. *Theoretical Computer Science 25*, 95–169.

De Nicola, R. and Hennessy, M. 1984. Testing equivalences for processes. *Theoretical Computer Science 34*, 83–133.

De Nicola, R. and Hennessy, M. 1987. CCS without *τ*'s. In *TAPSOFT/CAAP'87*. LNCS 249. Springer, 138–152.

De Nicola, R. and Labella, A. 2003. Nondeterministic regular expressions as solutions of equational systems. *Theor. Comput. Sci. 302,* 1-3, 179–189.

Derrick, J., Bowman, H., Boiten, E., and Steen, M. 1996. Comparing LOTOS and Z refinement relations. In *FORTE/PSTV'96*. Chapman & Hall, Kaiserslautern, Germany, 501–516.

Di Cosmo, R. 1995. *Isomorphisms of Types: from Lambda Calculus to Information Retrieval and Language Design*. Birkhäuser.

Fallside, D. C. and Walmsley, P. 2004. *XML Schema Part 0: Primer Second Edition*. W3C Recommendation, http://www.w3.org/TR/xmlschema-0/.

Fournet, C. and Gonthier, G. 1996. The reflexive chemical abstract machine and the join-calculus. In *Proceedings of the 23rd ACM Symposium on Principles of Programming Languages*. ACM, St. Petersburg Beach, Florida, 372–385.

Fournet, C., Gonthier, G., Lévy, J.-J., Maranget, L., and Rémy, D. 1996. A calculus of mobile agents. In *CONCUR*. Lecture Notes in Computer Science, vol. 1119. Springer, 406–421.

Fournet, C., Hoare, C. A. R., Rajamani, S. K., and Rehof, J. 2004. Stuck-free conformance. In *CAV'04*. LNCS 3114. Springer.

Gay, S. and Hole, M. 2005. Subtyping for session types in the π-calculus. *Acta Informatica 42,* 2-3, 191–225.

Hennessy, M. 1985. Acceptance trees. *Journal of the ACM 32,* 4, 896–928.

Hennessy, M. 1988. *Algebraic Theory of Processes*. Foundation of Computing. MIT Press.

Honda, K. 1993. Types for dyadic interaction. In *CONCUR '93*. LNCS 715. Springer, 509–523.

Honda, K., Vasconcelos, V. T., and Kubo, M. 1998. Language primitives and type discipline for structured communication-based programming. In *European Symposium on Programming*. LNCS 1381. Springer.

Laneve, C. and Padovani, L. 2006. Smooth orchestrators. In *FoSSaCS* (2006-04-05), L. Aceto and A. Ingólfsdóttir, Eds. LNCS, vol. 3921. Springer, 32–46.

Laneve, C. and Padovani, L. 2007. The *must* preorder revisited – An algebraic theory for web services contracts. In *18th International Conference on Concurrency Theory*. LNCS 4703, Springer.

Milner, R. 1982. *A Calculus of Communicating Systems*. Springer.

OCaml. Objective Caml. http://caml.inria.fr/ocaml/.

Rittri, M. 1993. Retrieving library functions by unifying types modulo linear isomorphism. *RAIRO Theoretical Informatics and Applications 27,* 6, 523–540.

Soloviev, S., Jones, A., and Luo, Z. 1996. Some Algorithmic and Proof-Theoretical Aspects of Coercive Subtyping. In *TYPES'96*. LNCS 1512, 173–196, Springer.

Takeuchi, K., Honda, K., and Kubo, M. 1994. An interaction-based language and its typing system. In *Parallel Architectures and Languages Europe*. 398–413.