Modular Semantics for Transition System Specifications with Negative Premises

Martin Churchill[1], Peter D. Mosses[1], and Mohammad Reza Mousavi[2]

[1] Department of Computer Science, Swansea University
{m.d.churchill,p.d.mosses}@swansea.ac.uk
[2] Halmstad University and Eindhoven University of Technology
m.r.mousavi@hh.se

Abstract. Transition rules with negative premises are needed in the structural operational semantics of programming and specification constructs, such as priority and interrupt, as well as in timed extensions of specification languages. The well-known proof-theoretic semantics for transition system specifications involving negative premises is based on well-supported proofs for closed transitions. However, such a semantics is inherently non-modular, in that proofs are not necessarily preserved by disjoint extensions of the transition system specification.
We conservatively extend the notion of well-supported proof to open transition rules. We prove that the resulting semantics is modular, consistent, and closed under instantiation. Our results provide the foundations for modular notions of bisimulation such that equivalence can be proved with reference only to the relevant rules, without appealing to all existing closed instantiations of terms.

1 Introduction

The main goal of this paper is to provide *modular* proof theory for structural operational semantics when transition rules with negative premises are allowed. The main technical contributions are a notion of well-supported proof for open transition rules, together with theorems that establish various essential properties of this notion. This is part of our larger research effort in defining a modular semantic framework, including machinery such as bisimulation proof techniques [14], and rule formats for the operational semantics of programming and specification languages which ensure that bisimilarity is a congruence [6].

When Plotkin introduced structural operational semantics (SOS) in his seminal Aarhus lecture notes in 1981 [16], he used only positive transition rules: the possibility of a transition for a programming construct depended on the possibility of transitions for its sub-constructs – never on their impossibility. In that context, the transition relation defined by a set of SOS rules is always well-defined, and the proof theory of transitions is quite straightforward (except regarding modularity of bisimilarity; see [14]). Positive transition rules are adequate for specifying the SOS of many programming and specification language constructs.

Nevertheless, negative premises have been found useful in SOS. For example, when termination can be conflated with deadlock (as in some process algebras) the following transition rules specify sequential execution of the construct $(x; y)$:

$$\frac{x \xrightarrow{l} x'}{(x; y) \xrightarrow{l} (x'; y)} \qquad \frac{x \overset{l'}{\nrightarrow} \quad y \xrightarrow{l} y'}{(x; y) \xrightarrow{l} y'}$$

This avoids the need to introduce distinguished terminal states, or a termination predicate.

More significantly, it has been shown [3] that transition rules with negative premises are actually *necessary* for the SOS of some programming and specification constructs, such as priority operators: SOS is strictly more expressive when negative premises are allowed. Related examples where negative premises are needed include interrupts and timed extensions of specification languages.

The model- and proof-theoretic semantics for SOS specifications involving negative premises is considerably less obvious than in the positive case; see [12,2,11] for detailed discussions and comparison of alternative definitions. A widely accepted definition is based on *well-supported proofs* for transition formulae $p \xrightarrow{l} q$ where p (and q) are *closed* terms [11]. Well-supported-proofs for open formulae has remained an open problem since 1995 [10] (and the task was characterised as 'somewhat problematic' by Van Glabbeek [11]). In the negative setting, the usual *closed-instance semantics* for open formulae would allow $r \overset{l}{\nrightarrow}$ to be inferred whenever it is impossible to infer $r \xrightarrow{l} u$ for any u (corresponding to 'negation as failure' in logic programming [7]). But this is inherently *non-modular*: proofs are not generally preserved when the transition system specification is extended with new constructs and with rules defining the transitions of the new constructs. The non-modularity stems from defining the notion of well-supported proof with respect to the set of all closed terms in a language: extensions of the specified language increase that set.

In this paper, we conservatively extend the notion of well-supported proof to *open transition rules*, in contrast to closed-instance semantics. We prove that the resulting semantics is modular, consistent, and closed under instantiation.

The conservativeness of our semantics requires a mild condition on the format of transition rules: *source-dependency*, which (informally stated) ensures that each variable in a rule can be traced back to variables that occur in the source of the conclusion (via transitions in the premises of the rule). Source-dependency was also required to show that disjoint extensions are operationally conservative with respect to closed transition formulae in [9]. Our other results (including modularity) apply to arbitrary specifications.

The work here provides foundations for modular notions of bisimulation for systems with negative premises, whereby equivalence between two terms can be proved with reference only to the rules that define transitions for the constructs occurring in those terms (independently of the presence or absence of other constructs and their defining rules). Modular bisimulation proofs correspond

closely to conventional proofs which appeal to the fact that 'no further rules need to be considered'.

The rest of this paper is organised as follows. In Section 2, we recall some standard notions. In Section 3, we generalise the notion of well-supported proof to open transition rules. We show that our notion of well-supported proof is consistent (i.e., does not lead to proofs of denying formulae) and closed under instantiation of formulas and transition rules. In Section 4, we study the issue of modularity. First, we show that the usual notion of closed instance semantics is not modular, in general. Second, we show that our approach to assigning semantics to open formulae is indeed modular. In Section 5, we show that our notion of semantics is a conservative extension of the existing notion for closed terms (i.e., it leads to the same set of provable transitions for closed terms), and that disjoint extensions are conservative. This requires the mild condition of source-dependency. We conclude the paper and present some direction for future work in Section 6.

2 Preliminaries

We begin by recalling some standard definitions regarding SOS specifications from the literature (see [2,15] for further details).

Definition 1 (Signatures, Terms and Substitutions) *We assume a countable set V of* variables*. A* signature Σ *is a set of function symbols with fixed arities; the arity of f is a non-negative integer denoted by $ar(f)$. The set of* terms *on signature Σ, denoted by $\mathbb{T}(\Sigma)$ and ranged over by $s, t, s_0, t_0, \ldots$, is defined inductively as follows: variables and function symbols of arity zero (also called constants) are terms; given a list of terms, their composition using a function symbol (while respecting the arity of the function symbol) is a term. Terms are also called* open terms*; the set of variables in t is denoted by $\mathsf{vars}(t)$.* Closed terms *on signature Σ, denoted by $\mathbb{C}(\Sigma)$ and ranged over by $p, q, \ldots$, are those terms in $\mathbb{T}(\Sigma)$ that do not contain any variable. A* substitution $\sigma : V \to \mathbb{T}(\Sigma)$ *is a function from variables to terms; it is* closing *if it maps variables to closed terms. These are lifted to functions on terms in the usual manner. We write ι for the identity substitution, and if σ is a substitution, write $\sigma[x \mapsto s]$ for the substitution that sends x to s and other variables y to $\sigma(y)$.*

Transition System Specifications (TSSs), introduced in [13,5], are formalisations of SOS specifications. Here, we consider TSSs where positive formulae are restricted to labelled transitions $s \xrightarrow{l} t$; extension to allow multiple transition relations and other predicates would be straightforward.

Definition 2 (Transition System Specification) *A* transition system specification T *is a tuple (Σ, L, D) where Σ is a signature, L is a set of labels (with typical members $a, b, a_0, \ldots$) and D is a set of deduction rules. For all $l \in L$, and $t, t' \in \mathbb{T}(\Sigma)$ we define that $t \xrightarrow{l} t'$ is a* positive formula *and $t \xnrightarrow{l}$ is a* negative

formula*; t is the* source *of both formulae and t' is the* target *of the former. A* formula *is either a positive or a negative formula. For each t, t', the formula $t \stackrel{a}{\not\rightarrow}$* denies *$t \xrightarrow{a} t'$ and vice versa. A formula is* closed *when all terms appearing in it are closed. A* deduction rule *$d \in D$ is a pair (H, ϕ), where H is a set of formulae and ϕ is a positive formula; ϕ is called the* conclusion *and the formulae from H are called the* premises*. A deduction rule is f-*defining *when the head operator of the source of its conclusion is f. A deduction rule is an* axiom *when its set of premises is the empty set, and* closed *when all formulae appearing in it are closed.*

We sometimes refer to a TSS by its set of deduction rules. A deduction rule (H, ϕ) is also written as $\frac{H}{\phi}$; in the latter syntax, if H is empty then it may be omitted.

We next recall the standard notion of proofs in TSSs with negative premises [11], to be generalised to open terms in the rest of this paper.

Definition 3 (Derivation) *A* derivation *π for $\frac{H}{\phi}$ in a TSS T is a well-founded upwardly branching tree with nodes labelled by formulae of T and of which*

- *the root is labelled by ϕ;*
- *if a node is labelled by ψ and the nodes immediately above it form the set K then:*
  - *$\psi \in H$ and $K = \emptyset$, or*
  - *ψ is a positive formula and $\frac{K}{\psi}$ is a substitution instance of a deduction rule in T.*

A derivation is closed *if all nodes are labelled with a closed formula. A formula* occurs in *a derivation if it labels a node in that derivation. We lift the application of substitutions to derivations in the usual way.*

Definition 4 (Provable Rule) *A closed deduction rule $\frac{H}{\phi}$ is a* provable rule *if it has a closed derivation π.*

Definition 5 (Ground Well-Supported Proof) *If ϕ is a closed formula, a* ground well-supported proof for *ϕ in a TSS T is a well-founded upwardly branching tree with nodes labelled by closed formulae and of which*

- *the root is labelled by ϕ;*
- *if a node is labelled by ψ and the nodes immediately above it form the set K then:*
  - *ψ is a positive formula and $\frac{K}{\psi}$ is an instance of a deduction rule in T, or*
  - *ψ is a negative formula and, for each set N of closed negative formulae and each ψ' denying ψ such that $\frac{N}{\psi'}$ is a provable rule, there is a formula in N denying a formula in K.*

The above definition corresponds to Definition 12 in [11].

3 Well-Supported Proofs

In this section, we generalise the notion of well-supported proof from closed formulae to *open rules*.

3.1 Provable Ruloids and Well-Supported Proofs

In order to build up a proof tree for $\frac{H}{\phi}$, one must provide justification for the to-be-proven formulae, until reaching a premise in H. For the positive formulae in such a proof tree, we require them to be justified using the deduction rules in the TSS. For the negative formulae, we consider *provable ruloids*: a generalisation of the notion of provable rule from closed to open rules.

Definition 6 (Provable Ruloid) *A context is a set* $\{x_i \xrightarrow{l_i} s_i, t_j \overset{l_j}{\nrightarrow} \mid i \in I, j \in J\}$ *of formulae (for possibly empty sets of indices* I *and* J*). A deduction rule* $\frac{H}{\phi}$ *is a* provable ruloid *if* H *is a context and* $\frac{H}{\phi}$ *has a derivation* π*. We say that* π witnesses *the provable ruloid* $\frac{H}{\phi}$*. A derivation* π *is a* provable ruloid derivation *if it witnesses some provable ruloid, i.e., each leaf with a positive formula has a variable as its source.*

The arbitrary negative formulas appearing in contexts and leaf positions of provable ruloid derivations correspond to the set N in Definition 5.

We next generalise the definition of well-supported proof to the open setting, under presence of a set of hypotheses asserting the possibility or impossibility of transitions from variables (so-called GSOS [4] contexts). We may discharge proof obligations for a negative formula by appealing to an appropriate hypothesis or by denying its possible proofs. In the open setting, such possible proofs may conclude substitutive instances of the formula in question.

Definition 7 (Well-Supported Proof) *A context* H *is called a GSOS context if the source of each formula in* H *(in particular, the negative ones) is a variable. For a GSOS context* H *and formula* ϕ*, a* well-supported proof *for* $\frac{H}{\phi}$ *in a TSS* T *is a well-founded upwardly branching tree with nodes labelled by formulae and of which*

- *the root is labelled by* ϕ*;*
- *if a node is labelled by* ψ *and the nodes immediately above it form the set* K *then:*
  - $\psi \in H$ *and* $K = \emptyset$*, or*
  - ψ *is a positive formula and* $\frac{K}{\psi}$ *is an instance of a deduction rule in* T*, or*
  - ψ *is a negative formula and for each substitution* σ*,* ψ' *denying* $\sigma(\psi)$ *and provable ruloid derivation* π *concluding* ψ'*, there exists* $\kappa \in K$ *and* κ' *denying* $\sigma(\kappa)$ *occurring in* π*.*

If $\frac{H}{\phi}$ has a well-supported proof, we write that $\frac{H}{\phi}$ is *(ws-)provable*. A well-supported proof is *closed* if it contains only closed formulae.

Remark 8 *In any TSS, $\overline{x \overset{l}{\not\rightarrow}}$ does not have a well-supported proof. For suppose it did, and consider the smallest such proof, with conclusion $x \overset{l}{\not\rightarrow}$ and immediate premises K. Then $x \overset{l}{\longrightarrow} x$ denies $\iota(x \overset{l}{\not\rightarrow})$, and $\frac{x \overset{l}{\longrightarrow} x}{x \overset{l}{\longrightarrow} x}$ is a provable ruloid, witnessed by a derivation π with a single node $x \overset{l}{\longrightarrow} x$. Hence there exists $\kappa \in K$ and κ' denying $\iota(\kappa) = \kappa$ occurring in π. But the only formula κ' occurring in π is $x \overset{l}{\longrightarrow} x$ and we must have $\kappa = x \overset{l}{\not\rightarrow}$. Hence, there exists another (smaller) proof for $\overline{x \overset{l}{\not\rightarrow}}$ in the original proof; this contradicts the assumption that we started from the smallest such proof.*

The above fact is crucial for modularity: the TSS may be extended with new constructs (and rules for them) which violate the general formula $x \overset{l}{\not\rightarrow}$, and we wish the old proofs to remain valid as the TSS is extended. In other words, the notion of negative proof search used in our notion of well-supported proof does not admit exhaustive case analysis on the possible instantiations of the variables.

Our definition of well-supported proof (Definition 7) differs from the closed notion (Definition 5) in some important respects, as illustrated by the following examples. However, in Section 5 we will show that for closed ϕ in a source-dependent TSS, $\overline{\phi}$ is ws-provable if and only if $\overline{\phi}$ has a ground well-supported proof.

Example 9 *Consider a TSS with unary symbols f, g; constants 0 and 1; label a; and deduction rules $\frac{f(x) \overset{a}{\not\rightarrow}}{g(x) \overset{a}{\longrightarrow} x}$, $\overline{f(0) \overset{a}{\longrightarrow} 0}$. Then:*

- *$\overline{f(1) \overset{a}{\not\rightarrow}}$ is provable as there are no provable ruloids concluding $\sigma(f(1) \overset{a}{\longrightarrow} y)$. Thus, $\overline{g(1) \overset{a}{\longrightarrow} 1}$ is also provable.*
- *Since $\overline{f(0) \overset{a}{\longrightarrow} 0}$ is a provable ruloid derivation, neither $\overline{f(0) \overset{a}{\not\rightarrow}}$ nor $\overline{g(0) \overset{a}{\longrightarrow} 0}$ are provable.*
- *$\overline{f(x) \overset{a}{\not\rightarrow}}$ is not provable, due to the provable ruloid derivation $\overline{f(0) \overset{a}{\longrightarrow} 0}$ concluding $\iota[x \mapsto 0](f(x) \overset{a}{\longrightarrow} 0)$. Thus, $\overline{g(x) \overset{a}{\longrightarrow} x}$ is not provable.*

The above example demonstrates why we must consider counterexamples up to substitution: otherwise, $\overline{f(x) \overset{a}{\not\rightarrow}}$ and $\overline{g(x) \overset{a}{\longrightarrow} x}$ would indeed be provable, but $\overline{g(0) \overset{a}{\longrightarrow} 0}$ unprovable – provability would not be closed under instantiation, which is counter-intuitive.

Example 10 *Consider a TSS with constant 0, unary f, labels a and b, and deduction rule $\frac{x \overset{a}{\longrightarrow} 0}{f(x) \overset{b}{\longrightarrow} 0}$. Then $\frac{x \overset{a}{\not\rightarrow}}{f(x) \overset{b}{\not\rightarrow}}$ is provable. Each ϕ that denies $\sigma(f(x) \overset{b}{\not\rightarrow})$*

is of the form $\sigma(f(x) \xrightarrow{b} s)$ *and the only provable ruloid derivation concluding this is* $\dfrac{\sigma(x) \xrightarrow{a} 0}{f(\sigma(x)) \xrightarrow{b} 0}$. *But* $\sigma(x \xrightarrow{a} 0)$ *occurs in this derivation, denying* $\sigma(x \overset{a}{\not\to})$, *as required.*

If we extend the TSS with an additional symbol 1 *with* $\overline{1 \xrightarrow{a} 0}$ *then* $\dfrac{x \overset{a}{\not\to}}{f(x) \overset{b}{\not\to}}$ *remains provable. This time, if* $\sigma(x) = 1$, *there is an additional provable ruloid derivation concluding* $\sigma(f(x) \xrightarrow{b} s)$ *to consider:* $\dfrac{\overline{1 \xrightarrow{a} 0}}{f(1) \xrightarrow{b} 0}$. *But* $1 \xrightarrow{a} 0$ *occurs in this provable ruloid, which denies* $\sigma(x \overset{a}{\not\to})$, *as required.*

The above example demonstrates why in Definition 7 we must allow κ' to occur in a non-leaf position of π. Otherwise, the proof of $\dfrac{x \overset{a}{\not\to}}{f(x) \overset{a}{\not\to}}$ would become invalid after extending by an unrelated constant 1, and modularity would fail.

Unlike the closed case, the provable ruloid derivations we consider may have positive leaves whose source is a variable. This is to allow negative information about variables to pass from the well-supported proofs to the provable ruloids. One might consider restricting negative leaves to those whose source is a variable (i.e., to GSOS contexts), but this would lead to an inconsistent notion of proof, as the next example shows.

Example 11 *Consider the TSS with the signature containing constant* 0, *unary function symbol* f, *label* a, *and deduction rule* $\dfrac{x \overset{a}{\not\to}}{f(x) \xrightarrow{a} f(x)}$.

Then $\overline{f^{2n+1}(0) \xrightarrow{a} f^{2n+1}(0)}$ *is provable for each* $n \in \mathbb{N}$, *by a simple induction on* n.

Now, consider the formula $f^3(0) \overset{a}{\not\to}$; *in order to prove it, one needs to find all provable ruloid derivations concluding* $f^3(0) \xrightarrow{a} t$ *(for some term* t*) and deny an occurring formula in each and every derivation. The only provable ruloid derivation with* $f^3(0) \xrightarrow{a} t$ *as its conclusion is* $\dfrac{f^2(0) \overset{a}{\not\to}}{f^3(0) \xrightarrow{a} f^3(0)}$. *Thus, if one only allowed provable ruloid derivations from GSOS contexts,* $\overline{f^3(0) \overset{a}{\not\to}}$ *would be provable as well as* $\overline{f^3(0) \xrightarrow{a} f^3(0)}$, *and consistency would fail.*

In the rest of this paper, we show that Definition 7 supports instantiation closure, consistency, modularity, and that (under the mild but necessary condition of source-dependency) disjoint extensions are conservative.

3.2 Basic Results

We first show that our notion of well-supported proof is consistent: it cannot be the case that both $\overline{\phi}$ and $\overline{\phi'}$ have well-supported proofs for denying ϕ and ϕ'. Since proofs for open formulae occur with respect to GSOS contexts, we generalise this notion of consistency to "consistent" contexts, i.e., contexts that do not

themselves lead to contradiction. In addition, the TSS should satisfy a sanity condition: it should not induce non-trivial deduction rules concluding formulae whose conclusion source is a variable. If it did, this can lead to contradiction when combined with GSOS contexts as proof hypotheses. For example, in a TSS with deduction rule $\dfrac{}{x \xrightarrow{l} x}$, any assumption of the form $x \overset{l}{\not\to}$ yields inconsistency – both $\dfrac{x \overset{l}{\not\to}}{x \overset{l}{\not\to}}$ and $\dfrac{x \overset{l}{\not\to}}{x \xrightarrow{l} x}$ have well-supported proofs. (In such pathological systems, consistency can still be recovered under positive GSOS contexts.) These requirements are captured in the following two definitions.

Definition 12 (Consistent Contexts) *A GSOS context is* consistent *if for each x, l, s, it does not contain both $x \xrightarrow{l} s$ and $x \overset{l}{\not\to}$.*

Definition 13 (Lean TSSs) *A TSS is* lean *if for variables x, $\dfrac{H}{x \xrightarrow{l} s}$ is only provable when $x \xrightarrow{l} s \in H$.*

Now, we have the ingredients to recast the consistency result in the setting with open terms.

Theorem 14 (Consistency) *Consider a TSS $T = (\Sigma, L, D)$ and consistent GSOS context H. Suppose further that T is lean,* or *H contains only positive formulae. Let ϕ and ϕ' be denying formulae. Then it is not the case that both $\dfrac{H}{\phi}$ and $\dfrac{H}{\phi'}$ have well-supported proofs.*

Proof. Assume that both ϕ and ϕ' are provable from H by well-supported proofs π and π' respectively. Assume without loss of generality that ϕ' is a negative formula. We will seek a contradiction, proceeding by induction on the total depth of π and π'.

If π' appeals to a hypothesis, then $\phi' \in H$ and so T must be lean. Then ϕ' is of the form $x \overset{l}{\not\to}$ and ϕ of the form $x \xrightarrow{l} s$. But π is a proof of $\dfrac{H}{\phi}$, and so by leanness $\phi \in H$. This contradicts consistency of H.

Otherwise, the root of π' is a negative deduction step. Now, construct a provable ruloid derivation π_1 from π by replacing all subtrees concluding negative $t \overset{l}{\not\to}$ by the leaf $t \overset{l}{\not\to}$. Then π_1 is a provable ruloid derivation concluding ϕ, which denies $\iota(\phi')$. Hence, there is a formula ψ occurring in π_1 and ψ' a premise of ϕ' in π', such that ψ denies $\iota(\psi') = \psi'$. Let π_2 denote the subproof of π rooted at ψ, and π_3 the subproof of π' rooted at ψ'. But then π_2 and π_3 are proofs of denying formulae, and are smaller than π and π' respectively; by the Inductive Hypothesis, this is impossible. □

The following result shows that the set of provable formulae is closed under instantiation.

Theorem 15 (Closure under Instantiating Formulae) *Consider a formula ϕ, contexts H and K, and substitution σ. Suppose $\frac{H}{\phi}$ has a well-supported proof and that for each $\psi_i \in H$, $\frac{K}{\sigma(\psi_i)}$ has a well-supported proof. Then $\frac{K}{\sigma(\phi)}$ has a well-supported proof.*

Corollary 16 *(i) If $\overline{\phi}$ is ws-provable, then so is $\overline{\sigma(\phi)}$. (ii) If $\overline{\phi}$ is provable and ϕ is closed, then $\overline{\phi}$ has a closed well-supported proof.*

The following theorem states that our notion of well-supported proof is preserved under instantiation of deduction rules in the TSS.

Theorem 17 (Closure under Instantiating Deduction Rules) *Consider a TSS $T = (\Sigma, L, D)$ and a set of deduction rules $D' \subseteq D$; let T' be $(\Sigma, L, D \cup \{\sigma_d(d) \mid d \in D'\})$, where σ_d is an arbitrary substitution for each $d \in D'$. Then a deduction rule $\frac{H}{\phi}$ is provable with respect to T if and only it is provable with respect to T'.*

The proofs are omitted due to lack of space and will be included in a forthcoming technical report.[3]

4 Modularity

4.1 Closed Instance Semantics

One can assign meaning to open formulae in a TSS via *closed-instance semantics*. This instantiates the deduction rules by all possible closed substitutions and considers the resulting formulae provable from the closed TSS.

Definition 18 (Closed-Instance Semantics) *Given a TSS $T = (\Sigma, L, D)$, closed(T) is defined as $(\Sigma, L, \{\sigma(d) \mid d \in D, \sigma : V \to \mathbb{C}(\Sigma)\})$, i.e., the set of deduction rules obtained by applying all closed substitutions on the deduction rules in D. The closed-instance semantics of a TSS T is the set of all closed formulae ϕ that have a ground well-supported proof with respect to closed(T).*

In such a setting, an open formula ϕ holds in T if and only if for all closed substitutions σ, $\sigma(\phi)$ has a ground well-supported proof in *closed*(T). The following example demonstrates that this does not coincide with ϕ having a well-supported proof in our setting.

Example 19 (Closed-Instance Semantics) *Consider TSS T_0 with constant 0, unary function f, labels a, b and deduction rule $\frac{x \overset{b}{\nrightarrow}}{f(x) \overset{a}{\longrightarrow} x}$. For each closed term p, there is a ground well-supported proof in closed(T_0) for the deduction rule $\overline{f(p) \overset{a}{\longrightarrow} p}$; hence, according to the closed-instance semantics, $f(x) \overset{a}{\longrightarrow} x$ holds. However, by Remark 8 there is no well-supported proof for $\overline{x \overset{b}{\nrightarrow}}$ in T_0, and so no well-supported proof of $\overline{f(x) \overset{a}{\longrightarrow} x}$.*

[3] For reviewers' convenience the proofs are gathered in a separate appendix.

For closed-instance semantics, a formula ϕ may hold in T_0 while failing in some *disjoint extension* [14] $T_0 \uplus T_1$ – closed-instance semantics is not *modular*.

Definition 20 (Disjoint Extension) *Consider two TSSs* $T_0 = (\Sigma_0, L_0, D_0)$ *and* $T_1 = (\Sigma_1, L_1, D_1)$ *of which the signatures agree on the arity of the shared function symbols. The* extension *of* T_0 *with* T_1*, denoted by* $T_0 \cup T_1$*, is defined as* $(\Sigma_0 \cup \Sigma_1, L_0 \cup L_1, D_0 \cup D_1)$*.* $T_0 \cup T_1$ *is a* disjoint *extension of* T_0 *when each deduction rule in* T_1 *is* f*-defining for some* $f \in \Sigma_1 \setminus \Sigma_0$*.*

Example 21 (Non-modularity of Closed-Instance Semantics) *Consider the TSS given in Example 19 and extend it by constant* 1 *with deduction rule* $\overline{1 \xrightarrow{b} 1}$*. Then there is no (ground) well-supported proof for* $\overline{f(1) \xrightarrow{a} 1}$ *and hence,* $\overline{f(x) \xrightarrow{a} x}$ *no longer holds for closed-instance semantics.*

4.2 Modularity for Well-supported Proofs

In contrast, we can show that well-supported proofs are modular: well-supported proofs in T_0 remain so in $T_0 \uplus T_1$.

In the following results, by abusing the notation, we write $s \in T$ to mean s is a term in the signature of TSS T. Similarly, we write $\phi \in T$ to denote that ϕ is a formula comprising terms and labels from T. For a substitution σ, $\sigma \in T$ indicates that for all x, $\sigma(x) \in T$. We will require the following lemma for factorising substitutions:

Lemma 22 *Let* $T_0 \uplus T_1$ *be a disjoint extension of* T_0*. Let* ϕ *be a formula in* $T_0 \uplus T_1$*, and* ψ, ω *be formulae in* T_0*. Let* $\sigma, \tau \in T_0 \uplus T_1$ *be substitutions such that* $\sigma(\psi) = \tau(\omega) = \phi$*. Then there exists substitutions* $\hat{\sigma} \in T_0$*,* $\hat{\tau} \in T_0$ *and* $\rho \in T_0 \uplus T_1$ *such that* $\sigma = \rho \circ \hat{\sigma}$*,* $\tau = \rho \circ \hat{\tau}$ *and* $\hat{\sigma}(\omega) = \hat{\tau}(\psi)$*.*

We first show that each provable ruloid deduction in $T_0 \uplus T_1$ whose conclusion is an instance of a T_0-formula can be approximated by a provable ruloid deduction in T_0. We do this using the following definition of "at the root" derivation, which approximates another derivation by proving the same conclusion from a possibly richer context.

Definition 23 (At The Root Derivation) *A derivation* ϕ *is* at the root *of a derivation* ψ *if the root node of* ϕ *is the root node of* ψ*, and any immediate subproof of* ϕ *is at the root of an immediate subproof of* ψ*.*

For example, $\dfrac{x \xrightarrow{a} w}{f(x,y) \xrightarrow{b} g(w,z)}$ is at the root of $\dfrac{x \xrightarrow{a} w \quad y \xrightarrow{a} z}{f(x,y) \xrightarrow{b} g(w,z)}$.

Lemma 24 (Provable Ruloid Approximation) *Let* $T_0 \uplus T_1$ *be a disjoint extension of* T_0*. Suppose* π *is a provable ruloid derivation in* $T_0 \uplus T_1$ *concluding* ϕ *with* $\phi = \sigma(\psi)$ *for* $\sigma \in T_0 \uplus T_1$ *and* $\psi \in T_0$*. Then there exists substitutions* $\tau \in T_0$*,* $\overline{\tau} \in T_0 \uplus T_1$ *with* $\sigma = \overline{\tau} \circ \tau$*, and a provable ruloid derivation* $\pi' \in T_0$ *concluding* $\tau(\psi)$ *such that* $\overline{\tau}(\pi')$ *is at the root of* π*.*

To obtain an approximating derivation in easy: let π' consist of a single hypothesis node ψ and set $\tau = \iota$ and $\overline{\tau} = \sigma$. But this is not a provable ruloid derivation: its hypothesis ψ may be positive but not have a variable at its source. The next lemma shows that given such an approximating derivation, one can improve it. Repeated application of this lemma then yields a provable ruloid derivation.

Lemma 25 *Under the hypotheses of Lemma 24, suppose further that $\sigma = \overline{\tau} \circ \tau$ with $\tau \in T_0$ and $\pi' \in T_0$ concludes $\tau(\psi)$ with $\overline{\tau}(\pi')$ at the root of π. Suppose that π' has a positive hypothesis (leaf) whose source is not a variable. Then there exists $\tau_1 \in T_0$, $\overline{\tau}_1$ with $\sigma = \overline{\tau}_1 \circ \tau_1$ and $\pi'_1 \in T_0$ concluding $\tau_1(\psi)$ such that $\overline{\tau}_1(\pi'_1)$ is at the root of π, with π'_1 strictly larger than π'.*

Proof. By assumption, there exists a hypothesis χ in π' at position P of the form $s \xrightarrow{l} s'$ where s is not a variable. Then $\overline{\tau}(\chi) = \overline{\tau}(s \xrightarrow{l} s')$ appears in π. This cannot be a hypothesis of π, as $\overline{\tau}(s)$ is not a variable and π is a provable ruloid derivation. Hence, $\overline{\tau}(\chi)$ must appear in π as the conclusion of a deduction rule d under substitution ρ (from premises ϕ_i). Rule d must occur in T_0 since $T_0 \uplus T_1$ is a disjoint extension of T_0 and the head symbol of $\overline{\tau}(s)$ is the head symbol of s and so in T_0. Suppose $d = \dfrac{\{\omega_i : i \in I\}}{\omega}$ with $\overline{\tau}(\chi) = \rho(\omega)$ and $\phi_i = \rho(\omega_i)$. Since ω and χ are both in T_0 we may apply Lemma 22 to obtain $\hat{\tau}, \hat{\rho} \in T_0$ and $\overline{\tau}_1$ with $\overline{\tau} = \overline{\tau}_1 \circ \hat{\tau}$, $\rho = \overline{\tau}_1 \circ \hat{\rho}$ and $\hat{\tau}(\chi) = \hat{\rho}(\omega)$. Let π'_1 be $\hat{\tau}(\pi')$ attached to $\hat{\rho}(d)$ at P and let $\tau_1 = \hat{\tau} \circ \tau$. Then π'_1 concludes $\tau_1(\psi) = \hat{\tau} \circ \tau(\psi)$. Also, $\overline{\tau}_1(\pi'_1)$ is at the root of π, as $\overline{\tau}_1(\hat{\tau}(\pi')) = \overline{\tau}(\pi')$ and $\overline{\tau}_1(\hat{\rho}(\omega_i)) = \rho(\omega_i) = \phi_i$. □

Proof of Lemma 24. First, set $\tau_0 = \iota$, $\overline{\tau}_0 = \sigma$ and π'_0 the derivation consisting of a single (hypothesis) node ψ. We then repeatedly apply Lemma 25 obtaining τ_i, $\overline{\tau}_i$, π'_i until some π'_j is a provable ruloid. This process terminates, as each π_i strictly increases in size, but does not exceed the size of π. We then set $\pi' = \pi'_j$, $\tau = \tau_j$ and $\overline{\tau} = \overline{\tau}_j$. □

Using Lemma 24, we next show that well-supported proofs are preserved by disjoint extensions.

Theorem 26 (Modularity for Well-Supported Proofs) *Suppose $T_0 \uplus T_1$ is a disjoint extension of T_0 and let π be a well-supported proof (resp. derivation) for $\dfrac{H}{\phi}$ in T_0. Then π is a well-supported proof (resp. derivation) for $\dfrac{H}{\phi}$ in $T_0 \uplus T_1$.*

Proof.
Derivations: Each derivation in T_0 is also a derivation in $T_0 \uplus T_1$. This follows from a straightforward induction, as each deduction rule in T_0 is also a deduction rule in $T_0 \uplus T_1$.
Well-supported proofs: We proceed by induction on π. If the derivation just appeals to a hypothesis, then it is also valid in $T_0 \uplus T_1$. If the root formula ϕ is positive and the derivation applies an instance of a deduction rule of T_0 to obtain sub-derivations $\{\pi_i : i \in I\}$ above ϕ, then we may apply the inductive

hypothesis to the nodes above ϕ and apply the same instance of the deduction rule to see that π is a proof in $T_0 \uplus T_1$.

If ϕ is negative and π has root $\frac{\{\psi_i : i \in I\}}{s \overset{l}{\not\longrightarrow}}$, then we must show that for each provable ruloid derivation $\pi' \in T_0 \uplus T_1$ concluding $\sigma(s) \xrightarrow{l} s'$, there is a formula occurring in π' denying some $\sigma(\psi_i)$. Consider such a π' and fresh x occurring in no ψ_i, and let $\sigma' = \sigma[x \mapsto s']$. Then π' concludes $\sigma'(s \xrightarrow{l} x)$. Since $s \xrightarrow{l} x$ is a formula in T_0, we may apply Lemma 24 to construct τ, $\overline{\tau}$ and π'' as described with $\overline{\tau}(\pi'')$ at the root of π'. Derivation π'' is in T_0 and concludes $\tau(s \xrightarrow{l} x)$, which denies $\tau(s \overset{l}{\not\longrightarrow})$. Since π is a well-supported proof there is a formula ψ' occurring in π'' denying some $\tau(\psi_i)$. Then $\overline{\tau}(\psi')$ occurs in $\overline{\tau}(\pi'')$ and so in π', and denies $\overline{\tau}(\tau(\psi_i)) = \sigma'(\psi_i) = \sigma(\psi_i)$, as required. □

5 Conservativeness

5.1 Conservativeness for Disjoint Extensions

We next show that for *source-dependent* TSSs, a disjoint extension of a TSS does not introduce additional provable formulae from the original TSS. In [9], an analagous result is presented for closed terms in the more abstract setting of three-valued stable models. From there, we recall the notion of *source-dependency*:

Definition 27 (Source-Dependency) *Given a proof rule, the* source-dependent variables *are defined inductively as follows:*

- *All variables in the source of the conclusion are source-dependent.*
- *If all variables in the source of a premise are source-dependent, so are those in the conclusion of that premise.*

A rule is source-dependent *if all variables it mentions are. A TSS is* source-dependent *if all of its rules are.*

Theorem 28 (Conservativeness for Disjoint Extensions) *Let $T_0 \uplus T_1$ be a disjoint extension of T_0, where T_0 is source-dependent, and let $\phi \in T_0$. Let π be a well-supported proof (resp. derivation) for $\frac{H}{\phi}$ in $T_0 \uplus T_1$. Then π is a well-supported proof (resp. derivation) for $\frac{H}{\phi}$ in T_0.*

Proof. (Sketch) For derivations and positive steps in well-supported proofs, we proceed by an outer induction on the proof and an inner induction on the source-dependence measure. For negative steps in well-supported proofs, we can use Theorem 26 to see that any denying derivation in T_0 is also one in $T_0 \uplus T_1$. □

The following example demonstrates why source-dependency is necessary for the above result (it is violated by the occurrence of x):

Example 29 *Consider a TSS T_0 with constants 0 and 1, labels a and b, and rule $\frac{x \xrightarrow{b} 1}{0 \xrightarrow{a} 1}$. Let $T_0 \uplus T_1$ extend T_0 with constant 2 and rule $2 \xrightarrow{b} 1$. Then $\frac{}{0 \xrightarrow{a} 1}$ is provable in $T_0 \uplus T_1$ but not in T_0, while $0 \xrightarrow{a} 1$ is a formula of T_0.*

5.2 Conservativeness over Closed-Instance Semantics

We next consider how our notion of well-supported-proof relates to the original notion of ground well-supported proof [11]. We first show that if a closed formula has a well-supported proof in T, then it has a ground well-supported proof in $\mathit{closed}(T)$. To do this, we define the notion of strict proof, which requires that the premises of a negative formula may not involve negative non-GSOS formulae.

Definition 30 (Strict Well-Supported Proof) *A* strict well-supported proof *is one in which if a negative formula ϕ occurs above a negative formula ψ then the source of ϕ is a variable.*

Lemma 31 *If $\frac{\Gamma}{\phi}$ has a (closed) well-supported proof, then it has a strict (closed) well-supported proof.*

Theorem 32 (Soundness w.r.t ground well-supported proofs) *For each closed formula ϕ, if $\overline{\phi}$ has a well-supported proof in T, then $\overline{\phi}$ has a ground well-supported proof in $\mathit{closed}(T)$.*

Proof. If $\overline{\phi}$ has a well-supported proof, then by Corollary 16 it has a closed well-supported proof, and by Lemma 31 a strict closed well-supported proof π. We claim that π is a ground well-supported proof of $\overline{\phi}$ in $\mathit{closed}(T)$.

Each positive step in π is a closed instance of a deduction rule in T. This is a valid step in a ground well-supported proof in $\mathit{closed}(T)$.

For the negative case, suppose the root is $\frac{K}{\phi}$. Let π' witness provable rule $\frac{H}{\phi'}$ in $\mathit{closed}(T)$ where ϕ' denies ϕ. Then π' is also a provable ruloid derivation in T, concluding ϕ' which denies $\iota(\phi)$. Since π is a well-supported proof in T, there is some $\chi \in K$ and χ' occurring in π' where χ' denies $\iota(\chi) = \chi$. Since χ' occurs in π' it must be closed, and so the source of χ must be closed. Since the source of χ is not a variable, strictness of π ensures that it is positive, and χ' negative. Since negative χ' occurs in provable ruloid derivation π', it must occur as a leaf, with $\chi' \in H$. Thus we have found $\chi \in K$ and $\chi' \in H$ denying χ, as required. □

For the converse, we will require source-dependency. The following example show that without source-dependency, the converse implication does not hold.

Example 33 *Consider TSS T with constants 0 and 1, labels a and b, and deduction rule $\frac{x \xrightarrow{b} 1}{0 \xrightarrow{a} 1}$. In $\mathit{closed}(T)$, $\overline{0 \xnrightarrow{a}}$ has a ground well-supported proof as there are no provable rules concluding $0 \xrightarrow{a} s$. But it does not have a well-supported proof in T: the provable ruloid derivation $\frac{x \xrightarrow{b} 1}{0 \xrightarrow{a} 1}$ would require a well-supported proof of $\overline{x \xnrightarrow{b} 1}$, which does not exist by Remark 8.*

The following proposition and subsequent theorem show that in source-dependent systems the converse of Theorem 32 holds.

Proposition 34 *Consider a source-dependent TSS T. Let ϕ be a formula whose source is closed and let π be a derivation in T concluding ϕ. Then π is a derivation in closed(T).*

Theorem 35 (Conservativeness over Closed-Instance Semantics) *Consider a source-dependent TSS T. For each closed formula ϕ, if $\overline{\phi}$ has a ground well-supported proof with respect to closed(T), then $\overline{\phi}$ has a well-supported proof with respect to T.*

Proof. Let π be the derivation in *closed*(T) witnessing $\overline{\phi}$. We show that π is also a well-supported proof in T. Since there are no hypotheses to appeal to, the only cases we need to consider are the positive and negative deduction steps. For the positive steps, any instance of a proof rule in *closed*(T) is an instance of a proof rule in T.

For the negative case, suppose $\frac{K}{\phi}$ occurs in π with ϕ negative. Let π' witness a provable ruloid $\frac{H}{\phi'}$ where ϕ' denies $\sigma(\phi)$. Then ϕ is closed since π is a deduction in *closed*(T), and so $\sigma(\phi)$ and the source of ϕ' are closed. By Proposition 34, π' is a derivation in *closed*(T). Each leaf of π' is in context H and closed, so must be a negative formula. Thus π' witnesses the provable rule $\frac{H}{\phi'}$. Since ϕ' denies $\sigma(\phi)$ and the source of ϕ is closed, ϕ' denies ϕ. Since π is a ground well-supported proof, there is a hypothesis $\chi \in K$ with negative $\chi' \in H$ where χ' denies χ. Since χ is closed, χ' also denies $\sigma(\chi)$. Thus χ' occurs in π' and denies $\sigma(\chi)$ with $\chi \in H$, as required. □

6 Conclusions

In this paper, we introduced a notion of semantics for open terms with respect to transition system specifications with negative premises. This notion extends the traditional notions [5,11] (which were confined to closed terms) and enjoys a number of intuitive properties: consistency, closure under instantiation, modularity and conservativeness. Consistency means that no two denying formulae are provable. Closure under instantiation means that firstly, instantiating deduction rules does not change the set of provable formulae and secondly, the set of provable formulae is closed under applying substitutions. Modularity means that all provable open formulae remain provable under disjoint extensions of the transition system specification. Conservativeness means that firstly, disjoint extensions do not introduce new provable formulae from the original TSS and secondly, our notion of semantics leads to the same set of provable closed transition formulae as the traditional notion.

This research was initiated in our study of bisimulation for open terms in the expressive setting of transition system specifications (such as those of the (n)tyft/(n)tyxt [12], ntree [8] and PANTH [19] formats). Earlier results consider open notions of bisimilarity which remain sound under disjoint extensions for purely positive TSSs (e.g., [6,14,1,17,18]). The notion introduced and results

obtained in this paper enable extension to the more expressive setting with negative premises.

References

1. Aceto, L., Cimini, M., Ingólfsdóttir, A.: Proving the validity of equations in GSOS languages using rule-matching bisimilarity. MSCS 22(2), 291–331 (2012).
2. Aceto, L., Fokkink, W.J., Verhoef, C.: Structural operational semantics. In: Handbook of Process Algebra, Chapter 3. pp. 197–292. Elsevier, 2001
3. Aceto, L., Ingolfsdottir, A.: On the expressibility of priority. Inf. Process. Lett. 109(1), 83–85 (2008)
4. Bloom, B., Istrail, S., Meyer, A.R.: Bisimulation can't be traced. JACM 42(1), 232–268 (1995)
5. Bol, R., Groote, J.F.: The meaning of negative premises in transition system specifications. JACM 43(5), 863–914 (1996)
6. Churchill, M., Mosses, P.D.: Modular bisimulation theory for computations and values. In: Foundations of Software Science and Computation Structures. LNCS, vol. 7794, pp. 97–112. Springer (2013),
7. Clark, K.L.: Negation as failure. In: Proc. ADBT'77, pp. 293–322. Plemum Press (1978)
8. Fokkink, W.J., van Glabbeek, R.J.: Ntyft/ntyxt rules reduce to ntree rules. I&C 126(1), 1–10 (1996)
9. Fokkink, W.J., Verhoef, C.: A conservative look at operational semantics with variable binding. I&C 146(1), 24–54 (1998)
10. van Glabbeek, R.J.: The meaning of negative premises in transition system specifications II. Tech. Report, Stanford (STAN-CS-TN-95-16) (1995)
11. van Glabbeek, R.J.: The meaning of negative premises in transition system specifications II. JLAP 60-61, 229–258 (2004)
12. Groote, J.F.: Transition system specifications with negative premises. TCS 118(2), 263–299 (1993)
13. Groote, J.F., Vaandrager, F.W.: Structured operational semantics and bisimulation as a congruence. I&C 100(2), 202–260 (1992)
14. Mosses, P.D., Mousavi, M.R., Reniers, M.A.: Robustness of equations under operational extensions. In: Proc. EXPRESS'10. EPTCS, vol. 41, pp. 106–120 (2010)
15. Mousavi, M., Reniers, M.A., Groote, J.F.: SOS rule formats and meta-theory: 20 years after. TCS 373, 238–272 (2007)
16. Plotkin, G.D.: A structural approach to operational semantics. JLAP 60-61, 17–139 (2004)
17. Rensink, A.: Bisimilarity of open terms. I&C 156, 345–385 (2000)
18. de Simone, R.: Higher-level synchronizing devices in MEIJE-SCCS. TCS 37, 245–267 (1985)
19. Verhoef, C.: A congruence theorem for structured operational semantics with predicates and negative premises. Nord. J. of Comp. 2(2), 274–302 (1995)