

# Axiomatizing Bisimulation Equivalences and Metrics from Probabilistic SOS Rules<sup>★</sup>

Pedro R. D'Argenio<sup>1</sup>, Daniel Gebler<sup>2</sup>, and Matias David Lee<sup>1</sup>

<sup>1</sup> Universidad Nacional de Córdoba & CONICET, Argentina

<sup>2</sup> VU University Amsterdam, The Netherlands

**Abstract.** Probabilistic transition system specifications (PTSS) provide structural operational semantics for reactive probabilistic labeled transition systems. Bisimulation equivalences and bisimulation metrics are fundamental notions to describe behavioral relations and distances of states, respectively. We provide a method to generate from a PTSS a sound and ground-complete equational axiomatization for strong and convex bisimilarity. The construction is based on the method of Aceto, Bloom and Vaandrager developed for non-deterministic transition system specifications. The novelty in our approach is to employ many-sorted algebras to axiomatize separately non-deterministic choice, probabilistic choice and their interaction. Furthermore, we generalize this method to axiomatize the strong and convex metric bisimulation distance of PTSS.

## 1 Introduction

Structural operational semantics (SOS for short) [20] is a powerful tool to provide semantics to programming languages. In SOS, process behavior is described using transition systems and the behavior of a composite process is given in terms of the behavior of its components. Based on this technique, different meta-properties have been studied. They state general properties on process operations by only inspecting the format of the rules that define the semantics of this operator. Among them, congruence and other compositionality properties stand out. (See [19] for an overview.)

However, there are properties that are better understood from an axiomatic point of view, by regarding the language as a signature equipped with an equational theory (see e.g. [18,3]). This is a different way to understand the language that brings new insights on the behavior of its operators and processes. General properties, such as associativity, distributivity, or reduction to basic operators, or specific ones, can be easily derived with equational reasoning, which is also used for the verification of systems.

In [1], Aceto, Bloom and Vaandrager link these two approaches by providing an algorithm to derive an equational theory for any language whose semantics is defined in terms of SOS rules that meet the GSOS format [7]. This equational theory is sound and ground-complete for bisimulation equivalence [18]. For recent work in the area, see [2,11] and references therein.

---

<sup>★</sup> Supported by ANPCYT PICT 2012-1823, SeCyT-UNC 05/B497 and 05/BP02, Erasmus Mundus Action 2 Lot 13A EU Mobility Programme 2010-2401/001-001-EMA2 and EU 7FP grant agreement 295261 (MEALS).

The above mentioned results are set in traditional non-deterministic semantics. However, in the modeling and programming of systems, the interaction of non-determinism and probabilities arises naturally, for example, in the sampling of a random number or in the occurrence of an externally induced fault. Therefore, modeling and programming languages need to have operations whose semantics include probabilistic behavior.

For probabilistic languages, SOS theories have also been developed in which not only congruence properties are considered, but also non-expansiveness, which is a concept that arises naturally when measuring distances in the probabilistic behavior of two processes (see, e.g., [9,12] and references therein). Moreover, equational theories for probabilistic languages have been developed (see [5,15] and references therein).

In this work we lift the result of [1] to languages with probabilistic operations. The input of our algorithm is an SOS system (more precisely, a PTSS) in PGSOS format (actually, it is a generalization of the Segala-GSOS format [6]) and the output is a sound and ground-complete equational theory for strong bisimulation equivalence. Having this aim, we came across with additional contributions, more precisely:

1. In Sec. 3, we generalize the PGSOS format to two-sorted signatures in order to syntactically denote states and distributions. By doing so, operations can be parameterized on distributions, and moreover, we can neatly express open terms in the rules of the PTSS. While the syntax somehow resembles the alternating model of probabilistic processes, we continue the research line of [9,17,12] and let PTSS have models in Segala's probabilistic automata. We show that strong bisimulation equivalence [16] and convex bisimulation equivalence (also called probabilistic bisimulation) [21] are congruences for any operation whose semantics is defined in PGSOS format.
2. In Sec. 4, we provide an algorithm that takes a PGSOS system, and produces an equational theory that is sound and ground-complete for strong bisimulation equivalence. We show ground-completeness for semantically well-founded PGSOS systems, and we indicate how this result can be extended to arbitrary PGSOS. We show how our algorithm easily extends to derive a sound and ground-complete equational theories for convex bisimulation equivalence.
3. As a by-product we needed to define a two-sorted calculus for finite probabilistic processes equipped with two sound and ground-complete equational theories, one for each bisimulation equivalence. This calculus is adapted from [5]. (See Sec. 2.)
4. In Sec. 5, we provide an equational theory for the basic calculus that captures exactly the notion of (strong) bisimilarity metric [10]. The equational theory is sound in the sense that, whenever the equality between the distance of two processes and the distance of two other processes (or a particular value) can be calculated with the calculus, it can also be calculated semantically in the probabilistic transition system. We show that it is also ground-complete (i.e. the inverse implication holds for closed terms).
5. Also in Sec. 5, we modify the previous algorithm to derive a sound and ground-complete equational theory for bisimilarity metric from a given PGSOS system.

## 2 Preliminaries

Let  $S = \{s, d\}$  be a set denoting two sorts. States of the transition system will be of sort  $s \in S$  and distributions over states of sort  $d \in S$ . We let  $\sigma$  range over the sorts

in  $S$ . We write  $S$ -sorted families  $X$  as pairs  $(X_s, X_d)$  with the first element  $X_s$  denoting the member of sort  $s$  and the second element  $X_d$  denoting the member of sort  $d$ . An  $S$ -sorted signature is a structure  $(F, \text{ar})$ , where (i)  $F$  is a set of *function names*, and (ii)  $\text{ar}: F \rightarrow (S^* \times S)$  is the *arity function*. The rank of  $f \in F$  is the number of arguments of  $f$ , defined by  $\text{rk}(f) = n$  if  $\text{ar}(f) = \sigma_1 \dots \sigma_n \rightarrow \sigma$ . (We write “ $\sigma_1 \dots \sigma_n \rightarrow \sigma$ ” instead of “ $(\sigma_1 \dots \sigma_n, \sigma)$ ”). Function  $f$  is a *constant* if  $\text{rk}(f) = 0$ . To simplify the presentation we will write an  $S$ -sorted signature  $(F, \text{ar})$  as a pair of disjoint signatures  $(\Sigma, \Gamma)$  where  $\Sigma$  is the set of operations that map to  $s$  and  $\Gamma$  is the set of operations that map to  $d$ .

Let  $(\mathcal{V}, \mathcal{D})$  be an infinite set of  $S$ -sorted variables where  $\mathcal{V}, \mathcal{D}, F$  are all mutually disjoint. We use  $x, y, z$  (with possible sub- or sup-indexes) to range over  $\mathcal{V}$ ,  $\mu, \nu$  to range over  $\mathcal{D}$  and  $\zeta$  to range over  $\mathcal{V} \cup \mathcal{D}$ . The  $S$ -sorted set of  $\Sigma$ -terms over  $(V, D) \subseteq (\mathcal{V}, \mathcal{D})$ , notation  $(T(\Sigma, V), T(\Gamma, D))$ , is the smallest set satisfying: (i)  $V \subseteq T(\Sigma, V)$ , (ii)  $D \subseteq T(\Gamma, D)$ , (iii)  $f(t_1, \dots, t_{\text{rk}(f)}) \in T(\Sigma, V)$ , if  $\text{ar}(f) = \sigma_1 \dots \sigma_n \rightarrow \sigma$ ,  $\sigma = s$ ,  $t_i \in T(\Sigma, V)$  whenever  $\sigma_i = s$ , and  $t_i \in T(\Gamma, D)$  whenever  $\sigma_i = d$ , and (iv)  $f(t_1, \dots, t_{\text{rk}(f)}) \in T(\Gamma, D)$ , if instead  $\sigma = d$ .  $(T(\Sigma, \mathcal{V}), T(\Gamma, \mathcal{D}))$  is the set of all *open terms* and is denoted by  $(\mathbb{T}(\Sigma), \mathbb{T}(\Gamma))$ .  $(T(\Sigma, \emptyset), T(\Gamma, \emptyset))$  is the set of all *closed terms* and is denoted by  $(\mathbb{T}(\Sigma), \mathbb{T}(\Gamma))$ .  $\text{Var}(t) \subseteq (\mathcal{V}, \mathcal{D})$  denotes the  $S$ -sorted set of variables in term  $t$ . We let  $\xi$  range over terms of both sorts  $T(\Sigma) \cup T(\Gamma)$ .

Let  $\Delta(T(\Sigma))$  denote the set of all (discrete) probability distributions on  $T(\Sigma)$ . We let  $\pi$  range over  $\Delta(T(\Sigma))$  and  $\psi$  range over  $\Delta(T(\Sigma)) \cup T(\Gamma)$ . For each  $t \in T(\Sigma)$ , let  $\delta_t$  denote the *Dirac distribution*, i.e.,  $\delta_t(t) = 1$  and  $\delta_t(t') = 0$  if  $t$  and  $t'$  are not syntactically equal. For  $X \subseteq T(\Sigma)$  we define  $\pi(X) = \sum_{t \in X} \pi(t)$ . The convex combination  $\sum_{i \in I} p_i \pi_i$  of a family  $\{\pi_i\}_{i \in I}$  of probability distributions with  $p_i \in (0, 1]$  and  $\sum_{i \in I} p_i = 1$  is defined by  $(\sum_{i \in I} p_i \pi_i)(t) = \sum_{i \in I} (p_i \pi_i(t))$ .

We fix the signature to describe probability distributions of finite support by  $\Gamma_\Delta = (F_\Delta, \text{ar}_\Delta)$  with  $F_\Delta = \{\delta, \oplus_p \mid p \in \mathbb{Q} \cap (0, 1)\}$ , and  $\text{ar}_\Delta(\delta) = s \rightarrow d$  and  $\text{ar}_\Delta(\oplus_p) = dd \rightarrow d$ . Given an arbitrary  $S$ -sorted signature with  $\Sigma_s = (F_s, \text{ar}_s)$ , the operations that map to sort  $s$  and all function symbols in  $F_s$  and  $F_\Delta$  are disjoint. We define the *probabilistic lifting* of  $\Sigma_s$  as an  $S$ -sorted signature  $(\Sigma, \Gamma)$  with  $\Sigma = \Sigma_s$  and  $\Gamma = (F_d, \text{ar}_d)$  extending  $\Gamma_\Delta$  such that for each  $f \in F_s$  there is a new distinct function symbol  $\mathbf{f} \in F_d$  with  $\text{ar}(\mathbf{f}) = d \dots d \rightarrow d$  and  $\text{rk}(\mathbf{f}) = \text{rk}(f)$ . (Operators in boldface are probabilistically lifted.)

The algebra associated with a probabilistically lifted signature  $(\Sigma, \Gamma)$  is defined as follows. For sort  $s$ , it is the freely generated algebra  $T(\Sigma)$ . For sort  $d$ , it is defined by the carrier  $\Delta(T(\Sigma))$  and the following interpretation:  $\llbracket \delta(t) \rrbracket = \delta_t$  for  $t \in T(\Sigma)$ ,  $\llbracket \theta_1 \oplus_p \theta_2 \rrbracket = p \llbracket \theta_1 \rrbracket + (1-p) \llbracket \theta_2 \rrbracket$  for  $\theta_1, \theta_2 \in T(\Gamma)$ ,  $\llbracket \mathbf{f}(\theta_1, \dots, \theta_{\text{rk}(f)}) \rrbracket (f(\xi_1, \dots, \xi_{\text{rk}(f)})) = \prod_{\sigma_j = s} \llbracket \theta_j \rrbracket (\xi_j)$  if for all  $\sigma_j = d$ ,  $\theta_j$  and  $\xi_j$  are syntactically equal, and, in any other case,  $\llbracket \mathbf{f}(\theta_1, \dots, \theta_{\text{rk}(f)}) \rrbracket (t) = 0$ .

A *substitution* is an  $S$ -indexed family of maps  $(\rho_s, \rho_d): (\mathcal{V}, \mathcal{D}) \rightarrow (\mathbb{T}(\Sigma), \mathbb{T}(\Gamma))$ . A substitution is closed if it maps each variable to a closed term. A substitution extends to a mapping from terms to terms as usual.

### 3 Probabilistic Transition System Specifications

Probabilistic transition systems (PTSs) generalize labelled transition systems by allowing for probabilistic choices in the transitions. We consider non-deterministic PTSs

(Segala-type systems) [21] with countable state spaces. A *probabilistic labeled transition system* (PTS) is a triple  $(T(\Sigma), A, \rightarrow)$ , where  $\Sigma$  is a signature specifying only functions with target sort  $s$ ,  $A$  is a countable set of actions, and  $\rightarrow \subseteq T(\Sigma) \times A \times \mathcal{A}(T(\Sigma))$  is a transition relation. We write  $t \xrightarrow{a} \pi$  for  $(t, a, \pi) \in \rightarrow$ . Satisfaction is defined by  $\rightarrow \models t \xrightarrow{a} \pi$  if  $t \xrightarrow{a} \pi \in \rightarrow$ , and  $\rightarrow \not\models t \xrightarrow{a} \pi$  if  $t \xrightarrow{a} \pi \notin \rightarrow$  for all  $\pi \in \mathcal{A}(T(\Sigma))$ .

We specify PTSs by means of transition system specifications [20,7,14]. We generalize the probabilistic GSOS format of [6] with operators of sort  $s$  with arguments of either sort  $s$  or  $d$ . From now on,  $(\Sigma, \Gamma)$  denotes a probabilistically lifted signature.

**Definition 1 (PGSOS-rule).** A PGSOS-rule has the form:

$$\frac{\{x_i \xrightarrow{a_{i,m}} \mu_{i,m} \mid i \in I, m \in M_i\} \quad \{x_i \xrightarrow{b_{i,n}} \nu_{i,n} \mid i \in I, n \in N_i\}}{f(\zeta_1, \dots, \zeta_{\text{rk}(f)}) \xrightarrow{a} \theta}$$

with  $f \in F$  a function symbol,  $I, M_i, N_i$  are finite index sets,  $a_{i,m}, b_{i,n}, a \in A$  are actions,  $x_i \in \mathcal{V}$ ,  $\zeta_i \in \mathcal{V} \cup \mathcal{D}$ ,  $\mu_{i,m} \in \mathcal{D}$  are variables,  $\theta \in \mathbb{T}(\Gamma)$  a distribution term, and satisfying the following constraints:

1. all  $\mu_{i,m}$  and  $\zeta_j$ , for  $i \in I, m \in M_i$  and  $j \in \{1, \dots, \text{rk}(f)\}$ , are pairwise different;
2.  $\{x_i \mid i \in I\} \subseteq \{\zeta_1, \dots, \zeta_{\text{rk}(f)}\}$ ;
3.  $\text{Var}(\theta) \subseteq \{\mu_{i,m} \mid i \in I, m \in M_i\} \cup \{\zeta_1, \dots, \zeta_{\text{rk}(f)}\}$ .

A *probabilistic transition system specification* in PGSOS format (PTSS) is a structure  $P = (\Sigma, A, R)$  where  $\Sigma$  is a probabilistically lifted signature,  $A$  is a finite set of labels and  $R$  is a finite set of PGSOS rules. For any rule  $r \in R$ , literals above the line are called *premises*, notation  $\text{prem}(r)$ ; the literal below the line is called *conclusion*, notation  $\text{conc}(r)$ . Given a positive literal  $t \xrightarrow{a} \theta$  and a closed substitution  $\rho$ ,  $\llbracket t \xrightarrow{a} \theta \rrbracket_\rho$  denotes the transition  $\rho(t) \xrightarrow{a} \llbracket \rho(\theta) \rrbracket$ . For negative literals,  $\llbracket t \xrightarrow{a} \theta \rrbracket_\rho$  denotes  $\rho(t) \not\xrightarrow{a} \theta$ . A *supported model* of  $P$  is a PTS  $(T(\Sigma), A, \rightarrow)$  satisfying that  $t \xrightarrow{a} \pi \in \rightarrow$  iff there is a rule  $r \in R$  with a substitution  $\rho$  such that all premises of  $r$  hold, i.e.  $\rightarrow \models \llbracket \text{prem}(r) \rrbracket_\rho$ , and the conclusion instantiates to  $t \xrightarrow{a} \pi$ , i.e.  $\llbracket \text{conc}(r) \rrbracket_\rho = t \xrightarrow{a} \pi$ . Each PTSS has a supported model which is, moreover, unique.

A set  $X \subseteq T(\Sigma)$  is closed with respect to a binary relation  $R \subseteq T(\Sigma) \times T(\Sigma)$  if  $R(X) \subseteq X$  where  $R(X) = \{t' \in T(\Sigma) \mid \exists t \in X. t R t'\}$ . A relation  $R \subseteq T(\Sigma) \times T(\Sigma)$  on terms of sort  $s$  lifts to a relation  $\bar{R} \subseteq \mathcal{A}(T(\Sigma)) \times \mathcal{A}(T(\Sigma))$  on distributions over terms of sort  $s$  by  $\pi \bar{R} \pi'$  iff  $\pi(X) = \pi'(X)$  for all  $X \subseteq T(\Sigma)$  that are closed with respect to  $R$ .

**Definition 2 ([16]).** Let  $(T(\Sigma), A, \rightarrow)$  be a PTS. A symmetric relation  $R \subseteq T(\Sigma) \times T(\Sigma)$  is a strong bisimulation if whenever  $t R t'$  and  $t \xrightarrow{a} \pi$ , there exists a transition  $t' \xrightarrow{a} \pi'$  such that  $\pi \bar{R} \pi'$ . Strong bisimilarity  $\sim$  is defined as the union of all strong bisimulations.

The convex closure  $cl(D)$  of a set of distributions  $D \subseteq \mathcal{A}(T(\Sigma))$  is the least subset of  $\mathcal{A}(T(\Sigma))$  which contains  $D$  and is closed under convex combination. A combined transition  $t \xrightarrow{a}_c \pi$  is given whenever  $\pi \in cl(\{\pi' \mid t \xrightarrow{a} \pi'\})$ .

**Definition 3 ([21]).** Let  $(T(\Sigma), A, \rightarrow)$  be a PTS. A symmetric relation  $R \subseteq T(\Sigma) \times T(\Sigma)$  is a convex bisimulation if whenever  $t R t'$  and  $t \xrightarrow{a} \pi$ , there exists a combined transition

$t' \xrightarrow{a}_c \pi'$  such that  $\pi \overline{R} \pi'$ . Convex bisimilarity  $\sim_c$  is defined as the union of all convex bisimulations.

A crucial property of process description languages to ensure compositional modeling is the compatibility of process operators with the chosen behavioral relation. In algebraic terms the compatibility of an equivalence  $R$  with an operator  $f$  is expressed by the congruence property which is defined as  $f(\xi_1, \dots, \xi_{rk(f)}) R f(\xi'_1, \dots, \xi'_{rk(f)})$  whenever  $\xi_i R \xi'_i$  with  $\xi_i, \xi'_i \in T(\Sigma)$  if  $\sigma_i = s$  and  $\xi_i \overline{R} \xi'_i$  with  $\xi_i, \xi'_i \in T(\Gamma)$  if  $\sigma_i = d$ . The PGSOS rule format ensures that both strong and convex bisimilarity are congruences.

**Theorem 1.** *Let  $P = (\Sigma, A, R)$  be a PTSS in PGSOS format. Then, both strong and convex bisimilarity are congruences for all operators defined by  $P$ .*

## 4 Axiomatization of Bisimulation Equivalences

The technique to derive an axiomatization for PGSOS operators follows the same strategy as in [1]. It starts with a given axiomatization of a basic calculus which is a probabilistic extension of CCS similar to the one studied in [5]. Then, according to the rules, axioms are provided for any other operator so that these operators can be eliminated, in the sense that every closed term can be equated to another closed term in the basic calculus. To introduce these new axioms, operators are split in three classes: distinctive, smooth, and non-smooth. *Distinctive operators* are well-behaved operators that distribute with summation and the probabilistic operators  $\oplus_p$  and  $\delta$ . The defining rules for distinctive operators can be directly mapped into axioms. *Smooth operators* are a generalization of distinctive operators in the sense that the set of rules defining the semantics of a smooth operator can be split in disjoint sets, each one of them satisfying the conditions of distinctive operators. Thus a smooth operator can be represented as a non-deterministic sum of distinctive operators. For each *non-smooth operator*, a new smooth operator is introduced that, when properly instantiated, shows the same behavior as the original non-smooth operator. Precisely the equality between these terms is introduced as a new axiom. This section presents these results and provides an algorithm that, given a PTSS  $P$  in PGSOS format, generates an axiom system for all operators in  $P$  that is sound and ground-complete for strong bisimilarity. We close the section with an explanation on how the technique extends to convex bisimilarity.

**Axiomatizing Finite Probabilistic Trees.** Let  $\Sigma_{CCS}$  be the signature of the (recursion free) *basic probabilistic CCS* defined by constant 0 of sort  $s$ , binary operation  $+$  with  $\text{ar}(+) = ss \rightarrow s$  and prefix operators  $a$  with  $\text{ar}(a) = d \rightarrow s$  for all  $a \in A$ . We write  $a.\theta$  for  $a(\theta)$  with  $\theta \in \mathbb{T}(\Gamma)$ . The PTSS  $P_{CCS} = (\Sigma_{CCS}, A, R)$  is given by the following rules  $R$ :

$$\frac{}{a.\mu \xrightarrow{a} \mu} \quad \frac{x \xrightarrow{a} \mu}{x + y \xrightarrow{a} \mu} \quad \frac{y \xrightarrow{a} \mu}{x + y \xrightarrow{a} \mu} \quad (1)$$

A closed term  $t \in T(\Sigma)$  is in *normal form* if either  $t = 0$  or  $t = \sum_{i \in I} a_i.\theta_i$  with  $\theta_i \in T(\Gamma)$  in normal form. A closed term  $\theta \in T(\Gamma)$  is in normal form if  $\theta = \bigoplus_{i \in I} p_i \delta(t_i)$ , with  $t_i \in T(\Sigma)$  in normal form and  $\sum_{i \in I} p_i = 1$ . Here,  $\bigoplus_{i \in \{1..n\}} p_i \theta_i$  is a shorthand for  $\theta_1 \oplus \frac{p_1}{\sum_{j=1}^n p_j} (\theta_2 \oplus \frac{p_2}{\sum_{j=2}^n p_j} (\dots (\theta_{n-1} \oplus \frac{p_{n-1}}{\sum_{j=n-1}^n p_j} \theta_n) \dots))$ , and  $\sum_{i \in \{1..n\}} t_i$  is a shorthand for  $t_1 + \dots + t_n$ .

**Table 1.** Axiomatization of strong and convex bisimilarity of CCS

$x + y = y + x$	(N1)	$(\mu_1 \oplus_p \mu_2) + \mu_3 = (\mu_1 + \mu_3) \oplus_p (\mu_2 + \mu_3)$	(NP1)
$(x + y) + z = x + (y + z)$	(N2)	$\mu_1 + (\mu_2 \oplus_p \mu_3) = (\mu_1 + \mu_2) \oplus_p (\mu_1 + \mu_3)$	(NP2)
$x + 0 = x$	(N3)	$\delta(x) + \delta(y) = \delta(x + y)$	(NP3)
$x + x = x$	(N4)		
		$a.\mu_1 + a.\mu_2 = a.\mu_1 + a.\mu_2 + a.(\mu_1 \oplus_p \mu_2)$	(CC)
$\mu \oplus_p \mu = \mu$	(P1)		
$\mu_1 \oplus_p \mu_2 = \mu_2 \oplus_{1-p} \mu_1$	(P2)	$\mu_1 \oplus_{p_1} (\mu_2 \oplus_{\frac{p_2}{1-p_1}} \mu_3) = (\mu_1 \oplus_{\frac{p_1}{p_1+p_2}} \mu_2) \oplus_{p_1+p_2} \mu_3$	(P3)

Let  $E_{CCS}$  be the set of equations of Table 1 without equation CC. The axioms N1–N4 are standard for non-deterministic choice of reactive systems [18]. The axioms P1–P3 are standard for probabilistic choice [5]. Moreover, axioms NP1–NP3 allow one to normalize distribution terms in a similar way to the normalization of state terms by axioms N1–N4. The axiomatization of [5] did not require those axioms because distribution terms were assumed to be already in normal form.

Equational reasoning over many-sorted algebras [13] requires non-empty carrier sets. For  $E_{CCS}$  and all its following extensions this holds since  $0 \in T(\Sigma)$  and  $\delta(0) \in T(\Gamma)$ . A set of  $S$ -sorted equations  $E$  over signature  $\Sigma$  is a sound and ground-complete axiomatization of strong bisimilarity of  $P$  if for all  $t, t' \in T(\Sigma)$ ,  $E \vdash t = t'$  iff  $t \sim t'$ .

In order to show ground-completeness of  $E_{CCS}$  we require that the axiomatization is normalizing for both sort  $s$  and  $d$ , i.e. that for each closed term  $\xi \in T(\Sigma) \cup T(\Gamma)$  there is a closed term  $\xi' \in T(\Sigma) \cup T(\Gamma)$  in normal form such that  $E_{CCS} \vdash \xi = \xi'$ . The proof of the next lemma follows as usual by transforming the axiom system into a term rewriting system, showing that it is strongly normalizing modulo commutativity and associativity, and that the normal form is indeed of the expected form.

**Lemma 1.** *The axiom system  $E_{CCS}$  is normalizing.*

The proof of soundness for axioms involving state terms follows standard lines: for each axiom we find a bisimulation relation that shows its instances are valid with respect to bisimilarity. For axioms on distribution terms we prove that both sides of the equation represent exactly the same distribution. Ground-completeness is proven by first reducing to normal form and then showing that, for two bisimilar state terms in normal form, the transfer properties induce a proof using the axioms. Similarly, two distribution terms in normal form that represent the same distribution up to bisimulation, can be reduced to the same term using the axioms.

**Theorem 2.**  *$E_{CCS}$  is sound and ground-complete for strong bisimilarity.*

In order to derive axioms for systems with rules including negative premises, following [1], we introduce the family of one-step restriction operators  $\partial_H^1$ , where  $H \subseteq A$ ,  $\text{ar}(\partial_H^1) = s \rightarrow s$ , and whose semantics is given by

$$\frac{x \xrightarrow{a} \mu}{\partial_H^1(x) \xrightarrow{a} \mu} \quad a \notin H \quad (2)$$

**Table 2.** Axioms for  $\partial_H^1$ 

$\partial_H^1(x + y) = \partial_H^1(x) + \partial_H^1(y)$	(H1)	$\partial_H^1(0) = 0$	(H4)
$\partial_H^1(a.\mu) = a.\mu$ if $a \notin H$	(H2)	$\partial_H^1(\mu_1 \oplus_p \mu_2) = \partial_H^1(\mu_1) \oplus_p \partial_H^1(\mu_2)$	(H5)
$\partial_H^1(a.\mu) = 0$ if $a \in H$	(H3)	$\partial_H^1(\delta(x)) = \delta(\partial_H^1(x))$	(H6)

$\partial_H^1(t)$  represents the inability to perform any action  $a \in H$  in the next step, otherwise behaving as  $t$ . The signature  $\Sigma_{CCS^\circ}$  extends  $\Sigma_{CCS}$  with operators  $\partial_H^1$ .  $P_{CCS^\circ} = (\Sigma_{CCS^\circ}, A, R_{CCS^\circ})$  is the PTSS whose set of rules  $R_{CCS^\circ}$  extends  $R_{CCS}$  with the family of rules given in (2).

Let  $E_{CCS^\circ}$  extends  $E_{CCS}$  with equations in Table 2. H1–H4 are standard for the one-step restriction operator [1]. H5 and H6 propagate the one-step restriction operation to each single term in the support of a distribution. Hence, restriction distributes over probabilistic choices and Dirac embedding. Soundness of H1–H4 is proven in the same way as for the non-probabilistic case [1]. Soundness of H5 and H6 is proven by showing that both sides of each axiom represent exactly the same distribution.  $\partial_H^1$  can be eliminated in the sense that for each closed term  $\xi \in T(\Sigma_{CCS^\circ}) \cup T(\Gamma_{CCS^\circ})$  there is a closed term  $\xi' \in T(\Sigma_{CCS}) \cup T(\Gamma_{CCS})$  such that  $E_{CCS^\circ} \vdash \xi = \xi'$ . This can be proven by induction on the height of a term. (Notice that, when read from left to right, axioms H1, H5, and H6 “push” operator  $\partial_H^1$  inside the term, while axioms H2–H4, remove it.) Using elimination and Thm. 2, ground-completeness follow immediately.

**Theorem 3.**  $E_{CCS^\circ}$  is sound and ground-complete for strong bisimilarity.

**Probabilistically Lifted Operators.** The semantics of all probabilistically lifted operators is defined following the same scheme. Thus, the axioms for these operators are defined similarly regardless of whether the original operator is distinctive, smooth or non-smooth. There are actually two types of axioms that explain how a lifted operation interacts with the probabilistic operations  $\oplus_p$  and  $\delta$ .

**Definition 4.** Let  $f$  be an operator with arity  $\text{ar}(f) = \sigma_1 \dots \sigma_{\text{rk}(f)} \rightarrow s$ . We associate with  $f$  the axiom system  $E_f$  consisting of the following equations:

1. Probabilistic distributivity laws: For each position  $i$  of  $f$ , such that  $\sigma_i = s$ , and for each  $p \in \mathbb{Q} \cap (0, 1)$  we have the equations

$$f(\mu_1, \dots, \mu'_i \oplus_p \mu''_i, \dots, \mu_{\text{rk}(f)}) = f(\mu_1, \dots, \mu'_i, \dots, \mu_{\text{rk}(f)}) \oplus_p f(\mu_1, \dots, \mu''_i, \dots, \mu_{\text{rk}(f)})$$

2. Dirac distributivity laws: We have the equation

$$f(\theta_1, \dots, \theta_{\text{rk}(f)}) = \delta(f(\zeta_1, \dots, \zeta_{\text{rk}(f)}))$$

with  $\theta_i = \delta(\zeta_i)$ ,  $\zeta_i \in \mathcal{V}$  if  $\sigma_i = s$  and  $\theta_i = \zeta_i$ ,  $\zeta_i \in \mathcal{D}$  if  $\sigma_i = d$ .

The soundness of these laws follows immediately from the semantics of  $\oplus_p$ ,  $\delta$  and the lifted operator, and using rational arithmetic. (Rational arithmetic be completely axiomatized for ground terms, which are the only ones we use, see e.g. [8]).

**Smooth and Distinctive Operators.** A smooth rule is a rule that, whenever a variable is tested in a positive literal, then it is the only literal that tests that variable and the tested variable does not occur in the target of the conclusion. A smooth operator is an operator defined only by smooth rules. A distinctive operator is a smooth operator in which the hypotheses of each pair of rules differ in at least one literal.

**Definition 5.** A PGSOS rule is smooth if it has the form

$$\frac{\{x_i \xrightarrow{a_i} \mu_i \mid i \in I\} \quad \{x_j \xrightarrow{b_{j,n}} \nu \mid j \in J, n \in N_j\}}{f(\zeta_1, \dots, \zeta_{\text{rk}(f)}) \xrightarrow{a} \theta} \quad (3)$$

where  $I$  and  $J$  are disjoint sets s.t.  $I \cup J = \{i \in \{1, \dots, \text{rk}(f)\} \mid \zeta_i \in \mathcal{V}\}$ , and  $x_i \notin \text{Var}(\theta)$  if  $i \in I$ . An operator  $f$  is smooth if all its defining rules are smooth.

A smooth operator  $f$  is distinctive if (i) each  $f$ -defining rule tests the same set of arguments  $I$  positively, and (ii) for every two different  $f$ -defining rules there is some argument  $\zeta_i \in \mathcal{V}$  tested positively by both rules, but with a different action.

Notice that  $+$  is smooth, but it is not distinctive since, e.g.,  $x$  is tested positively in the first rule (actually, a set of rules), but not in the second one. Instead,  $\partial_H^1$  is distinctive.

We introduce a new operator that we will use in our examples. Assume that each action  $a$  may fail with probability  $p_a \in [0, 1)$ . In case of failure, the occurrence of  $a$  is ignored and the system remains in the same state, otherwise, it proceeds normally. The new operator  $\text{sc}(t)$  is a safe controller that minimizes the probability of failure of process  $t$ . Its semantics is given by the rules

$$\frac{x \xrightarrow{a} \mu \quad \{x \xrightarrow{b} \nu \mid p_b < p_a, p_a \neq 0\}}{\text{sc}(x) \xrightarrow{a} \delta(x) \oplus_{p_a} \text{sc}(\mu)}, \text{ if } p_a > 0 \quad \frac{x \xrightarrow{a} \mu}{\text{sc}(x) \xrightarrow{a} \text{sc}(\mu)}, \text{ if } p_a = 0$$

$\text{sc}$  is a variant of the ACP-style priority operator and it is not smooth since the rule on the left tests  $x$  in the positive literal but also in the negative literal, and, moreover,  $x$  appears in the target of the conclusion.

Let  $\text{pos}(r) = I$  (resp.  $\text{neg}(r) = J$ ) be those positions which are positively (resp. negatively) tested by rule  $r$  (considering  $r$  as in (3)). Let  $\text{pact}(r, i) = \{a_i \mid i \in I\}$  (resp.  $\text{nact}(r, i) = \{b_{i,n} \mid n \in N_i\}$ ) be those actions for which  $x_i$  is positively (resp. negatively) tested by rule  $r$ . Note that if  $N_i = \emptyset$  then  $\text{nact}(r, i) = \emptyset$ . A position  $i$  of operator  $f$  is *positive* if  $i \in \text{pos}(r)$  for all rules  $r$  defining  $f$ .

**Definition 6.** Let  $f$  be a distinctive operator with arity  $\text{ar}(f) = \sigma_1 \dots \sigma_{\text{rk}(f)} \rightarrow s$ . Let  $\zeta_i \in \mathcal{V}$  if  $\sigma_i = s$  and  $\zeta_i \in \mathcal{D}$  if  $\sigma_i = d$  for  $1 \leq i \leq \text{rk}(f)$ . We associate with  $f$  the axiom system  $E_f$  consisting of the following equations:

1. Non-deterministic distributivity laws: For each positive position  $i$  of  $f$ , we have

$$f(\zeta_1, \dots, \zeta_i' + \zeta_i'', \dots, \zeta_{\text{rk}(f)}) = f(\zeta_1, \dots, \zeta_i', \dots, \zeta_{\text{rk}(f)}) + f(\zeta_1, \dots, \zeta_i'', \dots, \zeta_{\text{rk}(f)})$$

2. Action laws: For each  $f$ -defining rule  $r$  (as in (3)), we have the equation

$$\rho(f(\zeta_1, \dots, \zeta_{\text{rk}(f)})) = a.\rho(\theta)$$

with  $\theta = \text{trgt}(r)$  the target of  $r$  and substitution  $\rho$  defined by

$$\rho(\zeta) = \begin{cases} a_i \cdot \mu_i & \text{if } \zeta = x_i \text{ with } i \in \text{pos}(r) \\ \partial_H^1(x_i) & \text{if } \zeta = x_i \text{ with } i \in \text{neg}(r) \text{ and } H = \text{nact}(r, i) \neq \emptyset \\ \zeta & \text{otherwise.} \end{cases}$$

3. Inaction laws: We have the equations

$$\rho(f(\zeta_1, \dots, \zeta_{\text{rk}(f)})) = 0$$

for all sort-respecting substitutions  $\rho$  mapping into terms of the form  $0$ ,  $x$ ,  $a \cdot \mu$ ,  $b \cdot \mu + x$ , or  $\mu$ , such that for every  $f$ -defining rule  $r$  there is some position  $i$  with sort  $\sigma_i = s$  satisfying one of the following conditions: (i) if  $i \in \text{pos}(r)$ , then either  $\rho(\zeta_i) = 0$  or  $\rho(\zeta_i) = a \cdot \mu_i$  with  $a \notin \text{pact}(r, i)$ , or (ii) if  $i \in \text{neg}(r)$ , then  $\rho(\zeta_i) = b \cdot \mu_i + x$  with  $b \in \text{nact}(r, i)$ .

The fact that all rules of a distinctive operator  $f$  test positively the same positions guarantees the soundness of the non-deterministic distributivity law. There is one action law for each rule of  $f$ . The action law describes the execution of an action by pushing the executing action to the “head” of the term. The conditions of its associated rule are properly encoded in each operand of  $f$ . Contrarily to the action law, an inaction law traverses every  $f$ -defining rule ensuring through the operands that at least one of the conditions of each rule does not hold.

Soundness of the axioms in  $E_f$  can be proven regardless of the PTSS containing operator  $f$  as long as the set of rules defining the semantics of  $f$  is the same for any PTSS. That is, if  $f$  is defined in a PTSS  $P$ ,  $E_f$  is sound for any disjoint extension of  $P$ .

**Definition 7.** Let  $P = (\Sigma, A, R)$  and  $P' = (\Sigma', A, R')$  be two PTSSs in PGSOS format.  $P'$  is a disjoint extension of  $P$ , notation  $P' \sqsupseteq P$ , iff  $\Sigma \subseteq \Sigma'$ ,  $R \subseteq R'$  and  $R'$  introduces no new rule for any operation in  $\Sigma$ .

Then, we have the following theorem.

**Theorem 4.** Let  $P = (\Sigma, A, R)$  be a PTSS in PGSOS format, s.t.  $P \sqsupseteq P_{\text{CCS}^\circ}$  and  $\Sigma_{sd} = \Sigma - \Sigma_{\text{CCS}^\circ}^\circ$  is a collection of distinctive operators. Let  $E_P$  be the axiom system consisting of  $E_{\text{CCS}^\circ}$  and  $E_f \cup E_f$ , for each  $f \in \Sigma_{sd}$ . Then, for every disjoint extension  $P' \sqsupseteq P$  in PGSOS format, the axiom system  $E_P$  is sound for strong bisimilarity on  $P'$ .

Notice that the set of rules  $R$  defining a smooth operator  $f$  in a PTSS  $P$  can always be partitioned into sets  $R_1, \dots, R_m$ , such that  $f$  is distinctive when considering only the rules in  $R_i$ . Let  $f_i$  be fresh operators with arity  $\text{ar}(f_i) = \text{ar}(f)$  and let  $R'_i$  be the same set of rule as  $R_i$  only that the operator in the source of each rules is renamed to  $f_i$ . Consider the disjoint extension  $P' \sqsupseteq P$  with all fresh operators  $f_i$  and rules in  $R'_1 \cup \dots \cup R'_m$  added to the signature and set of rules of  $P$ , respectively. Then, it should be clear that the distinctive law

$$f(\zeta_1, \dots, \zeta_{\text{rk}(f)}) = f_1(\zeta_1, \dots, \zeta_{\text{rk}(f)}) + \dots + f_m(\zeta_1, \dots, \zeta_{\text{rk}(f)}) \quad (4)$$

is sound for bisimilarity. Thus, a smooth operator  $f$  is axiomatized by the non-deterministic choice over the distinctive variants of  $f$ .

**Table 3.** Axiomatization of  $\mathbf{sc}$  (redundant laws, such as  $\overline{\mathbf{sc}}(0, a.\mu) = 0$ , are omitted)

$$\begin{array}{ll}
\overline{\mathbf{sc}}(x_1 + x_2, y) = \overline{\mathbf{sc}}(x_1, y) + \overline{\mathbf{sc}}(x_2, y) & \overline{\mathbf{sc}}(a.\mu, y) = a.\mathbf{sc}(\mu) \quad \text{if } p_a = 0 \\
\overline{\mathbf{sc}}(a.\mu, \delta_H^1(x)) = a.(\delta(\delta_H^1(x)) \oplus_{p_a} \mathbf{sc}(\mu)) & \overline{\mathbf{sc}}(0, y) = 0 \\
\quad \text{if } p_a > 0, \text{ with } H = \{b \mid p_b < p_a\} & \overline{\mathbf{sc}}(a.\mu, b.v + y) = 0 \quad \text{if } p_b < p_a \\
\overline{\mathbf{sc}}(\mu_1 \oplus_p \mu_2, \nu) = \overline{\mathbf{sc}}(\mu_1, \nu) \oplus_p \overline{\mathbf{sc}}(\mu_2, \nu) & \overline{\mathbf{sc}}(\delta(x), \delta(y)) = \delta(\overline{\mathbf{sc}}(x, y)) \\
\overline{\mathbf{sc}}(\mu, \nu_1 \oplus_p \nu_2) = \overline{\mathbf{sc}}(\mu, \nu_1) \oplus_p \overline{\mathbf{sc}}(\mu, \nu_2) & 
\end{array}$$

**Theorem 5.** *Let  $P = ((\Sigma, \Gamma), A, R)$  be a PTSS in PGSOS format, s.t.  $P \sqsupseteq P_{CCS^\partial}$  and  $f \in \Sigma$  be a smooth operator. There is a disjoint extension  $P' = ((\Sigma', \Gamma'), A, R')$  of  $P$  with  $m$  distinctive smooth operations  $f_1, \dots, f_m$  such that  $\mathbf{ar}(f_i) = \mathbf{ar}(f)$  for  $1 \leq i \leq m$  and (4) is sound for strong bisimulation in any disjoint extension of  $P'$ .*

**Non-smooth Operators.** An operator that is not smooth has a rule in which a variable that is tested in a positive literal either is tested in a second literal or it appears in the target of a conclusion. In this case we proceed by constructing a smooth version of the operator with one argument for each kind of use of the variable that breaks smoothness (actually, one argument for each positive test plus an additional one if the variable is tested negatively or it appears on the target of the conclusion of a rule). Thus, for the unary operator  $\mathbf{sc}$ , we introduce a binary operator  $\overline{\mathbf{sc}}$ , the first argument related to the positive literal and the other related to the negative test and the occurrence in the target of the rule. So  $\overline{\mathbf{sc}}$  is defined by the rules

$$\frac{x \xrightarrow{a} \mu \quad \{y \xrightarrow{b} \cdot \mid p_b < p_a\}}{\overline{\mathbf{sc}}(x, y) \xrightarrow{a} \delta(y) \oplus_{p_a} \mathbf{sc}(\mu)}, \text{ if } p_a > 0 \quad \frac{x \xrightarrow{a} \mu}{\overline{\mathbf{sc}}(x, y) \xrightarrow{a} \mathbf{sc}(\mu)}, \text{ if } p_a = 0$$

It should be clear that  $\mathbf{sc}(x) = \overline{\mathbf{sc}}(x, x)$ . Moreover, notice that  $\overline{\mathbf{sc}}$  is smooth. (In fact, it is also distinctive.) The premise on the second rule could have alternatively tested on  $y$  rather than  $x$ , in which case,  $\overline{\mathbf{sc}}$  would have also been smooth but not distinctive.

In general, given a non-smooth operator  $f$ , we define a new smooth operator  $f'$  by extending its arity as explained above, and proceeding as following: for each rule  $r$  of  $f$  we introduce a new rule  $r'$  for  $f'$  such that, if we intend to equate  $f(\vec{\zeta}) = f'(\vec{\zeta}')$ , and  $f(\vec{\zeta})$  and  $f'(\vec{\zeta}')$  are the sources of  $r$  and  $r'$ , respectively,  $r[\vec{\zeta}/\vec{\zeta}]$  and  $r'[\vec{\zeta}'/\vec{\zeta}']$  have to be identical with the exception of their sources. (Here,  $[\vec{\zeta}/\vec{\zeta}]$  denotes the usual substitution of variables.) Notice that this results in a one to one correspondence between the rules of  $f$  and those of  $f'$ . Then, we have the following theorem.

**Theorem 6.** *Let  $P$  be a PTSS in PGSOS format, s.t.  $P \sqsupseteq P_{CCS^\partial}$ . Let  $f \in \Sigma_P$  be a non-smooth operator. Then there is a disjoint extension  $P' \sqsupseteq P$  with a smooth operator  $f'$  s.t. the equation  $f(\zeta_1, \dots, \zeta_{\mathbf{rk}(f)}) = f'(\zeta'_1, \dots, \zeta'_{\mathbf{rk}(f)})$ , where  $\zeta_i$ ,  $1 \leq i \leq \mathbf{rk}(f)$  are all different variables and  $\{\zeta'_1, \dots, \zeta'_{\mathbf{rk}(f)}\} \subseteq \{\zeta_1, \dots, \zeta_{\mathbf{rk}(f)}\}$ , is sound for strong bisimulation in every disjoint extension of  $P'$ .*

As an example, we complete the axiomatization of  $\mathbf{sc}$  with the axioms for  $\overline{\mathbf{sc}}$  which can be derived using Definitions 4 and 5. They are given in Table 3.

As a result of the previous theorems, we obtain the algorithm of Fig. 1 that, given a PTSS  $P_i$  in PGSOS format, generates an equational theory  $E_o$  that captures the behavior of all operations in  $P_i$  and is sound for strong bisimilarity.

Input: a PTSS  $P_i$  in PGSOS format

Output: a PTSS  $P_o$  in PGSOS format, with  $P_o \sqsupseteq P_i$ , and an equational theory  $E_o$  that is sound for strong bisimilarity in all disjoint extensions of  $P_o$ .

1. If necessary, complete  $P_i$  so that it disjointly extends  $CCS^\delta$ .
2. For each non-smooth operator of  $P_i$ , extend the system with a smooth version according to Thm. 6 and add all the corresponding equations to  $CCS^\delta$ .
3. For each smooth non-distinctive operator  $f \notin \Sigma_{CCS^\delta}$  in the resulting PTSS, apply the construction of Thm. 5 and extend the PTSS with the distinctive operators  $f_1, \dots, f_m$  and the respective rules. Add also the resulting instances of axiom (4).
4. Add all equations associated to the distinctive operators in the resulting system (but not in  $\Sigma_{CCS^\delta}$ ) according to Def. 6.
5. Finally, for every operator not in  $\Sigma_{CCS^\delta}$  add the equation for their respective lifted version according to Def. 4.

**Fig. 1.** Algorithm to generate an axiomatization for  $P_i$

The fact that the set of rules of  $P_i$  (and hence also  $P_o$ ) is finite guarantees that the equational theory  $E_o$  is *head-normalizing* for all operations of  $P_o$ , that is, every closed term of  $P_o$  can be proven equal to a term of the form  $0$ ,  $\sum_{i \in I} a_i \cdot \theta_i$  or  $\bigoplus_{j \in J} p_j \delta(t_j)$ , with  $\theta_i \in T(\Gamma_{P_o})$  and  $t_j \in T(\Sigma_{P_o})$ , within the equational theory  $E_o$ . The construction of head-normal forms is the key towards proving ground-completeness. In fact, notice that if the semantics of a term  $t \in T(\Sigma_{P_o})$  is a finite tree, then all operators can be eliminated in  $E_o$  (i.e., there is a term  $t' \in T(\Sigma_{CCS})$ , s.t.,  $E_o \vdash t = t'$ ). However this is not the case in general. Consider the constant operator  $\text{nwf}$  whose semantics is defined by the rule  $\text{nwf} \xrightarrow{a} \delta(\text{nwf}) \oplus_{\frac{1}{2}} \delta(0)$ . Using the action law, axiom  $\text{nwf} = a \cdot (\delta(\text{nwf}) \oplus_{\frac{1}{2}} \delta(0))$  is derived, in which the elimination process will never terminate.

In order to guarantee ground-completeness, we adapt the notion of semantic well-foundedness of [1] to our setting. A term  $t \in T(\Sigma_P)$  is *semantically well founded* in  $P$  if there is no infinite sequence  $t_0 a_0 \theta_0 t_1 a_1 \theta_1 \dots$  of terms  $t_i \in T(\Sigma_P)$  and  $\theta_i \in T(\Gamma_P)$  and actions  $a_i \in A$ , such that  $t_i \xrightarrow{a_i} \theta_i$  is derivable in  $P$  and  $\llbracket \theta_i \rrbracket(t_{i+1}) > 0$ , for all  $i \geq 0$ .  $P$  is *semantically well founded* if all its terms are. Now, if  $P_o$  is semantically well founded (which is the case if  $P_i$  is semantically well-founded and  $P_i \sqsupseteq P_{CCS}$ ),  $E_o$  has an elimination theorem. As a consequence, we have the following theorem.

**Theorem 7.** *Let  $P_i$  be the input and  $P_o$  and  $E_o$  be the outputs of the algorithm in Fig. 1. If  $P_i$  is semantically well-founded with  $P_i \sqsupseteq P_{CCS}$ , then the equational theory  $E_o$  is ground-complete for strong bisimulation in  $P_o$ .*

Ground completeness can be extended to semantically non well-founded PTSS in PGSOS format by also using the approximation induction principle (AIP) [4]. We omit the details here. The proof follows closely the lines of [1].

**Axiomatization of Convex Bisimulation.** Equation CC of Table 1 was introduced in [5] which proved it sound for convex bisimilarity. The equational theory resulting from extending  $E_{CCS}$  with CC is ground-complete for  $CCS$  modulo convex bisimilarity. The proof of this result proceeds very much like the one in [5].

Since all the axioms generated by the algorithm in Fig. 1 are sound for strong bisimilarity, they are also sound for convex bisimilarity. Since they also provide elimination for semantically well founded terms, we have the following result:

**Theorem 8.** *Let  $P_i$  be a semantically well-founded PTSS in PGSOS format with  $P_i \sqsupseteq P_{CCS}$ . Let the PTSS  $P_o$  and the equational theory  $E_o$  be the outputs of the algorithm in Fig. 1. Then, (i)  $E_o \cup \{\text{CC}\}$  is sound for convex bisimulation in any disjoint extension of  $P_o$ , and (ii) it is ground-complete in  $P_o$ .*

## 5 Axiomatization of Bisimilarity Metric

In the previous section we developed an equational theory for bisimulation equivalence. Now we shift our focus to bisimilarity pseudometrics and develop an equational theory that characterizes the bisimulation distance.

**Axiomatization of Finite Probabilistic Trees.** A 1-bounded pseudometric on  $T(\Sigma)$  is a function  $d: T(\Sigma) \times T(\Sigma) \rightarrow [0, 1]$  such that (i)  $d(t, t) = 0$ ; (ii)  $d(t, t') = d(t', t)$ ; and (iii)  $d(t, t'') \leq d(t, t') + d(t', t'')$  for all  $t, t', t'' \in T(\Sigma)$ . Pseudometrics are used to formalize the notion of *behavioral distance* between terms.

A *matching*  $\omega \in \Delta(T(\Sigma) \times T(\Sigma))$  for  $(\pi, \pi') \in \Delta(T(\Sigma)) \times \Delta(T(\Sigma))$  is a distribution satisfying  $\sum_{t' \in T(\Sigma)} \omega(t, t') = \pi(t)$  and  $\sum_{t \in T(\Sigma)} \omega(t, t') = \pi'(t')$  for all  $t, t' \in T(\Sigma)$ . We denote by  $\mathcal{Q}(\pi, \pi')$  the set of all matchings for  $(\pi, \pi')$ . The *Kantorovich pseudometric*  $\mathbf{K}(d): \Delta(T(\Sigma)) \times \Delta(T(\Sigma)) \rightarrow [0, 1]$  lifts a pseudometric  $d: T(\Sigma) \times T(\Sigma) \rightarrow [0, 1]$  on state terms to distributions:

$$\mathbf{K}(d)(\pi, \pi') = \min_{\omega \in \mathcal{Q}(\pi, \pi')} \sum_{t, t' \in T(\Sigma)} d(t, t') \cdot \omega(t, t') \quad (5)$$

for  $\pi, \pi' \in \Delta(T(\Sigma))$ . Note that  $\mathbf{K}(d)(\delta_t, \delta_{t'}) = d(t, t')$  for all  $t, t' \in T(\Sigma)$ . The *Hausdorff pseudometric*  $\mathbf{H}(\hat{d}): P(\Delta(T(\Sigma))) \times P(\Delta(T(\Sigma))) \rightarrow [0, 1]$  lifts a pseudometric  $\hat{d}: \Delta(T(\Sigma)) \times \Delta(T(\Sigma)) \rightarrow [0, 1]$  on distributions to *sets* of distributions:

$$\mathbf{H}(\hat{d})(\Pi_1, \Pi_2) = \max \left\{ \sup_{\pi_1 \in \Pi_1} \inf_{\pi_2 \in \Pi_2} \hat{d}(\pi_1, \pi_2), \sup_{\pi_2 \in \Pi_2} \inf_{\pi_1 \in \Pi_1} \hat{d}(\pi_2, \pi_1) \right\} \quad (6)$$

for  $\Pi_1, \Pi_2 \subseteq \Delta(T(\Sigma))$  whereby  $\inf \emptyset = 1$  and  $\sup \emptyset = 0$ .

**Definition 8 ([10]).** *Let  $(T(\Sigma), A, \rightarrow)$  be a PTS. A 1-bounded pseudometric  $d$  on  $T(\Sigma)$  is a bisimulation metric if for all  $t, t' \in T(\Sigma)$  with  $d(t, t') < 1$ , whenever there is a transition  $t \xrightarrow{a} \pi$  then there exists a transition  $t' \xrightarrow{a} \pi'$  such that  $\mathbf{K}(d)(\pi, \pi') \leq d(t, t')$*

We order bisimulation metrics  $d_1 \sqsubseteq d_2$  iff  $d_1(t, t') \leq d_2(t, t')$  for all  $t, t' \in T(\Sigma)$ . The smallest bisimulation metric, notation  $\mathfrak{d}$ , is called *bisimilarity metric* and assigns to each pair of processes their least possible distance. Strong bisimilarity is the kernel of the bisimilarity metric [10], i.e.  $\mathfrak{d}(t, t') = 0$  iff  $t \sim t'$ .

Let  $E_{CCS}^m$  be the system of equations in Table 4. The equations consider two kind of symbols for metrics: one on state terms (**d**) and the other on distribution terms (**δ**). Axioms D1–D4 correspond to conditions (i) and (ii) of the definition of a pseudometric. Axioms MN and MP lift the axioms for bisimulation to metrics. In a way, they state that two bisimilar terms should have the same distance to a third term. From Def. 8, it can be

**Table 4.** Axiomatization of bisimilarity metric of CCS. (We assume  $\min \emptyset = 1$ .)

$$\mathbf{d}(x, x) = 0 \quad (\text{D1}) \quad \mathbf{d}(\mu, \mu) = 0 \quad (\text{D3})$$

$$\mathbf{d}(x, y) = \mathbf{d}(y, x) \quad (\text{D2}) \quad \mathbf{d}(\mu, \nu) = \mathbf{d}(\nu, \mu) \quad (\text{D4})$$

$$\mathbf{d}(t, x) = \mathbf{d}(t', x) \quad \text{where } t = t' \text{ is one of axioms N1–N4} \quad (\text{MN})$$

$$\mathbf{d}(\theta, \mu) = \mathbf{d}(\theta', \mu) \quad \text{where } \theta = \theta' \text{ is one of axioms NP1–NP3 or P1–P3} \quad (\text{MP})$$

$$\mathbf{d}(0, a.\mu + x) = 1 \quad (\text{H1})$$

$$\mathbf{d}\left(\sum_{i \in I} a_i.\mu_i, \sum_{j \in J} b_j.\nu_j\right) = \max \left\{ \max_{i \in I} \min_{j \in J, a_i = b_j} \mathbf{d}(\mu_i, \nu_j), \max_{j \in J} \min_{i \in I, a_i = b_j} \mathbf{d}(\mu_i, \nu_j) \right\} \quad (\text{H2})$$

$$\mathbf{d}\left(\bigoplus_{i \in I} p_i \delta(x_i), \bigoplus_{j \in J} q_j \delta(y_j)\right) = \min_{\omega \in \Omega(I, J)} \sum_{i \in I, j \in J} \mathbf{d}(x_i, y_j) \cdot \omega(i, j) \quad (\text{K})$$

$$\text{where } \Omega(I, J) = \{\omega : I \times J \rightarrow [0, 1] \mid \forall i \in I : \omega(i, J) = p_i, \forall j \in J : \omega(I, j) = q_j\}$$

easily seen that  $d$  is a bisimulation metric whenever  $\max_{a \in A} \mathbf{H}(\mathbf{K}(d))(\{\pi \mid t \xrightarrow{a} \pi\}, \{\pi' \mid t' \xrightarrow{a} \pi'\}) \leq d(t, t')$ . This is captured by H1 and H2. The equality in the axioms is due to the fact that we aim to characterize only the bisimilarity metric  $\mathfrak{d}$ . Finally, axiom K corresponds to the definition of the Kantorovich pseudometric. We also need the following general rules that should be considered together with the usual inference rules of equational logic. For all  $f : \sigma_1 \dots \sigma_{\text{rk}(f)} \rightarrow s$  and  $g : \sigma_1 \dots \sigma_{\text{rk}(g)} \rightarrow d$ , we have

$$\frac{\{\mathbf{d}(\zeta_i, \zeta'_i) = 0, \mathbf{d}(\zeta_j, \zeta'_j) = 0 \mid 1 \leq i, j \leq \text{rk}(f), \sigma_i = s, \sigma_j = d\}}{\mathbf{d}(f(\zeta_1, \dots, \zeta_{\text{rk}(f)}), z) = \mathbf{d}(f(\zeta'_1, \dots, \zeta'_{\text{rk}(f)}), z)} \quad (\text{S1})$$

$$\frac{\{\mathbf{d}(\zeta_i, \zeta'_i) = 0, \mathbf{d}(\zeta_j, \zeta'_j) = 0 \mid 1 \leq i, j \leq \text{rk}(f), \sigma_i = s, \sigma_j = d\}}{\mathbf{d}(g(\zeta_1, \dots, \zeta_{\text{rk}(g)}), z) = \mathbf{d}(g(\zeta'_1, \dots, \zeta'_{\text{rk}(g)}), z)} \quad (\text{S2})$$

These rules ensure that  $E_{CCS}^m \vdash \mathbf{d}(t, t'') = \mathbf{d}(t', t'')$  whenever  $E_{CCS} \vdash t = t'$  and similarly for distribution terms.

Let  $\mathfrak{d}$  be the bisimilarity metric and  $\mathbf{K}(\mathfrak{d})$  its Kantorovich lifting. Let  $\rho$  be a closed substitution. We define  $\llbracket \mathbf{d}(t, t') \rrbracket_\rho = \mathfrak{d}(\rho(t), \rho(t'))$  and  $\llbracket \mathbf{d}(\theta, \theta') \rrbracket_\rho = \mathbf{K}(\mathfrak{d})(\llbracket \rho(\theta) \rrbracket, \llbracket \rho(\theta') \rrbracket)$  for  $t, t' \in \mathbb{T}(\Sigma_{CCS})$  and  $\theta, \theta' \in \mathbb{T}(\Gamma_{CCS})$ . We lift  $\llbracket \_ \rrbracket_\rho$  to arithmetic terms containing expressions of the form  $\mathbf{d}(t, t')$  or  $\mathbf{d}(\theta, \theta')$  in the obvious way (e.g.  $\llbracket \min_{i \in I} \text{expr}_i \rrbracket_\rho = \min_{i \in I} \llbracket \text{expr}_i \rrbracket_\rho$ ).  $E_{CCS}^m$  is sound for  $\mathfrak{d}$  in the sense that, whenever  $E_{CCS}^m \vdash \text{expr} = \text{expr}'$  (meaning that  $\text{expr} = \text{expr}'$  can be proved using axioms in  $E_{CCS}^m$  and arithmetic), then  $\llbracket \text{expr} \rrbracket_\rho = \llbracket \text{expr}' \rrbracket_\rho$  for every closed substitution  $\rho$ . Soundness should be clear for all the axioms except maybe for H2. By definition of bisimulation metric, the right-hand side is smaller than or equal to the left-hand side interpreting them on any closed substitution. Equality follows from the fact that  $\mathfrak{d}$  is the *smallest* bisimulation metric.

Besides,  $E_{CCS}^m$  is also ground-complete for  $\mathfrak{d}$ , in the sense that, for any (closed) arithmetic expressions  $\text{expr}$  and  $\text{expr}'$  possibly containing closed terms of the form  $\mathbf{d}(t, t')$  or  $\mathbf{d}(\theta, \theta')$  with  $t, t' \in \mathbb{T}(\Sigma_{CCS})$  and  $\theta, \theta' \in \mathbb{T}(\Gamma_{CCS})$ ,  $\llbracket \text{expr} \rrbracket = \llbracket \text{expr}' \rrbracket$  implies  $E_{CCS}^m \vdash \text{expr} = \text{expr}'$ . Notice that by arithmetic, this is a direct consequence of the following claims: (i) for all closed state terms  $t, t' \in \mathbb{T}(\Sigma_{CCS})$  and  $p \in [0, 1]$ , if  $\mathfrak{d}(t, t') = p$  then  $E_{CCS}^m \vdash \mathbf{d}(t, t') = p$ , and (ii) for all closed distribution terms  $\theta, \theta' \in \mathbb{T}(\Gamma_{CCS})$ , if  $\mathbf{K}(\mathfrak{d})(\llbracket \theta \rrbracket, \llbracket \theta' \rrbracket) = p$ ,  $E_{CCS}^m \vdash \mathbf{d}(\theta, \theta') = p$ . The proof of these claims follows by reducing closed terms involved in  $\mathbf{d}(t, t')$  and  $\mathbf{d}(\theta, \theta')$  to normal form using

axioms D1–D4, MN, and MP (and rules S1 and S2), and then inductively applying H1, H2, K and arithmetic calculations to reach the expected value.

**Theorem 9.**  $E_{CCS}^m$  is sound and ground-complete for the bisimilarity metric  $\mathfrak{d}$ .

**Axiomatization of Bisimilarity Metric of PGSOS.** The algorithm of Fig. 1 can be modified to provide axioms for bisimilarity metric to any operator defined in PGSOS as follows. Instead of adding the axioms in  $E_{CCS}$ , add the axioms in  $E_{CCS}^m$ , and for each equation  $t_1 = t_2$  (resp.  $\theta = \theta'$ ) added by the algorithm in Fig. 1, add instead  $\mathfrak{d}(t_1, x) = \mathfrak{d}(t_2, x)$  (resp.  $\mathfrak{d}(\theta, \mu) = \mathfrak{d}(\theta', \mu)$ ).

Soundness of the axioms introduced by the algorithm is straightforward: we know that  $t_1 \sim t_2$  implies  $d(t_1, t_2) = 0$  and hence  $d(t_1, t) = d(t_2, t)$  can be calculated from properties (ii) and (iii) in the definition of pseudometric (similarly for distribution terms).

We already observed that  $E_{CCS}^m$  is normalizing. Besides, it can be shown that the axiom system generated by the new algorithm is head-normalizing. Then, for every semantically well founded closed term  $t$  there is a  $t'$  in normal form such that  $\mathfrak{d}(t, t'') = \mathfrak{d}(t', t'')$  for every  $t''$ . Using this elimination result ground-completeness follows.

**Theorem 10.** Let  $P_i$  be a PTSS in PGSOS format and let the PTSS  $P_o$  and the equational theory  $E_o$  be the outputs of the algorithm in Fig. 1 modified as before. Then, (i)  $E_o$  is sound for the bisimilarity metric  $\mathfrak{d}$  in any disjoint extension of  $P_o$ , and (ii) it is ground-complete in  $P_o$ , provided  $P_o$  is semantically well founded.

## 6 Concluding Remarks

As we pointed out in [9], the use of literals as a triple  $t \xrightarrow{a} \theta$  in PTSS rules (rather than the old fashion quadruple  $t \xrightarrow{a,p} t'$  that partially specifies a probabilistic jump) paves the way for generalizing the theory transition system specification to the probabilistic setting. We went further in this paper and defined a two-sorted signature that leads to a rigorous and clear definition of the distribution term in the target of positive literals. Moreover, this also fits nicely with the introduction of the equational theory.

This setting allows us to borrow the strategies of [1] to obtain the algorithm of Fig. 1 and prove its correctness (Thm. 7). This is particularly facilitated by the introduction of the operators mapping into sort  $d$ , and particularly by the fact that all probabilistically lifted operators distribute with respect to  $\oplus_p$  and  $\delta$ . The generalization of the algorithm to behavioral equivalences weaker than strong bisimilarity and whose equational theories contain  $E_{CCS}$ , is simple as demonstrated with convex bisimilarity (Thm. 8).

The result that convex bisimilarity is a congruence for all operators defined with PGSOS rules (Thm. 1) is new in this paper and, to our knowledge, it is actually the first time that a general congruence theorem is proved for *convex* bisimilarity. Here, we insist on the advantages of a good definition: this result is a direct consequence of the fact that strong bisimilarity is a congruence and this is so because the definition of combined transition can be encoded with a set of PGSOS rules (then a strong bisimulation in the extended PTSS is also a convex bisimulation).

We remark that the axiomatization  $E_{CCS}^m$  of bisimilarity metric is new in this paper. Axiom scheme H2 can be translated into a set of axioms that only include binary sum

by introducing an auxiliary operator. However we have been unable so far to find a set of axioms that only use binary  $\oplus_p$  operators in order to replace the axiom scheme K.

## References

1. Aceto, L., Bloom, B., Vaandrager, F.: Turning SOS rules into equations. *Inf. Comput.* 111(1), 1–52 (1994)
2. Aceto, L., Goriac, E.-I., Ingolfssdottir, A., Mousavi, M.R., Reniers, M.A.: Exploiting algebraic laws to improve mechanized axiomatizations. In: Heckel, R. (ed.) *CALCO 2013*. LNCS, vol. 8089, pp. 36–50. Springer, Heidelberg (2013)
3. Baeten, J.C.M., Basten, T., Reniers, M.A.: *Process Algebra: Equational Theories of Communicating Processes*. Cambridge University Press, New York (2009)
4. Baeten, J.C.M., Bergstra, J.A., Klop, J.W.: On the consistency of Koomen’s fair abstraction rule. *TCS* 51, 129–176 (1987)
5. Bandini, E., Segala, R.: Axiomatizations for probabilistic bisimulation. In: Orejas, F., Spirakis, P.G., van Leeuwen, J. (eds.) *ICALP 2001*. LNCS, vol. 2076, pp. 370–381. Springer, Heidelberg (2001)
6. Bartels, F.: *On Generalised Coinduction and Probabilistic Specification Formats*. Ph.D. thesis, VU University Amsterdam (2004)
7. Bloom, B., Istrail, S., Meyer, A.R.: Bisimulation can’t be traced. *J. ACM* 42, 232–268 (1995)
8. Contejean, E., Marché, C., Rabehasaina, L.: Rewrite systems for natural, integral, and rational arithmetic. In: Comon, H. (ed.) *RTA 1997*. LNCS, vol. 1232, pp. 98–112. Springer, Heidelberg (1997)
9. D’Argenio, P.R., Lee, M.D.: Probabilistic transition system specification: Congruence and full abstraction of bisimulation. In: Birkedal, L. (ed.) *FOSSACS 2012*. LNCS, vol. 7213, pp. 452–466. Springer, Heidelberg (2012)
10. Desharnais, J., Jagadeesan, R., Gupta, V., Panangaden, P.: The metric analogue of weak bisimulation for probabilistic processes. In: *Proc. LICS 2002*, pp. 413–422. IEEE (2002)
11. Gazda, M., Fokkink, W.: Turning GSOS rules into equations for linear time-branching time semantics. *The Computer Journal* 56(1), 34–44 (2013)
12. Gebler, D., Tini, S.: Compositionality of approximate bisimulation for probabilistic systems. In: *Proc. EXPRESS/SOS 2013*. EPTCS, vol. 120, pp. 32–46 (2013)
13. Goguen, J.A., Meseguer, J.: Completeness of many-sorted equational logic. *SIGPLAN Not.* 17(1), 9–17 (1982)
14. Groote, J.F., Vaandrager, F.: Structured operational semantics and bisimulation as a congruence. *Inf. Comput.* 100, 202–260 (1992)
15. Hennessy, M.: Exploring probabilistic bisimulations, part I. *Formal Aspects of Computing* 24(4-6), 749–768 (2012)
16. Larsen, K.G., Skou, A.: Bisimulation through probabilistic testing. *Inf. Comput.* 94, 1–28 (1991)
17. Lee, M.D., Gebler, D., D’Argenio, P.R.: Tree rules in probabilistic transition system specifications with negative and quantitative premises. In: *Proc. EXPRESS/SOS 2012*. EPTCS, vol. 89, pp. 115–130 (2012)
18. Milner, R.: *Communication and Concurrency*. Prentice-Hall (1989)
19. Mousavi, M.R., Reniers, M.A., Groote, J.F.: SOS formats and meta-theory: 20 years after. *Theor. Comput. Sci.* 373(3), 238–272 (2007)
20. Plotkin, G.: A structural approach to operational semantics. Report DAIMI FN-19, Aarhus University (1981), reprinted in *J. Log. Algebr. Program.* 60-61, 17–139 (2004)
21. Segala, R.: *Modeling and Verification of Randomized Distributed Real-Time Systems*. Ph.D. thesis, MIT (1995)