Compositional Weak Metrics for Group Key Update

Ruggero Lanotte[1], Massimo Merro[2], and Simone Tini[3]

1 **Dipartimento di Scienze e Alta Tecnologia, Università dell'Insubria, Italy**
`ruggero.lanotte@uninsubria.it`
2 **Dipartimento di Informatica, Università degli Studi di Verona, Italy**
`massimo.merro@univr.it`
3 **Dipartimento di Scienze e Alta Tecnologia, Università dell'Insubria, Italy**

Abstract

We investigate the compositionality of both weak bisimilarity metric and weak similarity quasi-metric semantics with respect to a variety of standard operators, in the context of probabilistic process algebra. We show how compositionality with respect to nondeterministic and probabilistic choice requires to resort to rooted semantics. As a main application, we demonstrate how our results can be successfully used to conduct compositional reasonings to estimate the performances of group key update protocols in a multicast setting.

1998 ACM Subject Classification F.3.2 Semantics of Programming Languages

Keywords and phrases Behavioural metric, compositional reasoning, group key update

Digital Object Identifier 10.4230/LIPIcs.MFCS.2017.72

1 Introduction

Behavioural distances [35, 17, 14] allow us to compare the behaviour of probabilistic systems. Basically, they are the quantitative analog of the classical notions of *behavioural equivalence* and *preorder*. In the *weak semantic* approach, where *non-observable* actions are abstracted away, *weak bisimilarity metric* [18] and its asymmetric counterpart, *weak similarity quasi-metric* [30], have been proposed as the quantitative analog of *weak probabilistic bisimilarity* and *weak probabilistic similarity*, respectively [5, 4].

In order to specify and verify systems in a compositional manner, it is necessary to work with behavioural semantics which are preserved by all operators of the language. In this light, different forms of compositionality have been proposed for strong bisimilarity metrics by adopting different notions of *uniform continuity* [20]. Intuitively, a uniformly continuous operator ensures that a small variation in the behaviour of a system component leads to a smooth and bounded variation in the behaviour of the whole system (absence of chaotic behaviour when system components and parameters are modified in a controlled manner). More precisely, the uniform continuity of an n-ary process algebra operator f ensures that, once fixed the maximal tolerable distance ε between processes $f(s_1,\ldots,s_n)$ and $f(s'_1,\ldots,s'_n)$, there are values δ_i such that, whenever the distance between process arguments s_i and s'_i is below δ_i, for $1 \leq i \leq n$, then the distance between $f(s_1,\ldots,s_n)$ and $f(s'_1,\ldots,s'_n)$ is guaranteed to be below ε. The notions of uniform continuity considered in [20] are: (i) *non-extensiveness*, requiring $\varepsilon = \max(\delta_1,\ldots,\delta_n)$, (ii) *non-expansiveness*, with $\varepsilon = \delta_1+\ldots+\delta_n$, and (iii) *Lipschitz continuity*, where $\varepsilon = L\cdot(\delta_1+\ldots+\delta_n)$, for some $L \in \mathbb{R}_{\geq 1}$.

In this paper, we extend and generalise the work of [20] to *rooted* and *asymmetric* semantics. In particular, for all standard operators of probabilistic process algebras, such as

probabilistic CCS [24] and probabilistic CSP [24], we derive the notions of uniform continuity which are satisfied by *rooted* bisimilarity metric and/or *rooted* similarity quasimetric. It is well-known that weak probabilistic bisimilarity, unlike similarity, is not preserved by nondeterministic choice. Thus, with no surprise, the nondeterministic choice operator is not uniformly continuous with respect to weak bisimilarity metric, while it is uniformly continuous with respect to weak similarity quasimetric. In this paper, we show that probabilistic choice is uniformly continuous with respect to neither weak bisimilarity metric nor weak similarity quasimetric. Thus, in order to recover uniform continuity, we work with rooted (bi)similarities [36], where, in first step of the (bi)simulation game any *strong* transition must be matched by the same *strong* transition.

As main case study, we consider an abstract specification of the *group key update* protocol. In this protocol, whenever a principal joins or leaves the group, in order to guarantee *backward* and *forward confidentiality*, it is necessary to generate and distribute a new group key. However, this operation has a cost in terms of:

(i) the number of attacks aiming at compromising the group key,
(ii) the degradation of communication service,
(iii) battery consumption.

We show how our compositional theory can be used to estimate the distance between the ideal protocol, where groups cannot dynamically change, and some variations of the protocol obtained by playing with the following parameters:

(i) number of principals,
(ii) probability that principals leave the group,
(iii) probability that principals join the group.

The results of our analysis allow us to assert that the protocol under consideration has good efficiency in groups with low dynamicity, regardless of the size of the group.

Outline. Section 2 provides background on probabilistic semantics. Section 3 contains the main results on uniform continuity. Section 4 applies our theory to an abstract group key update protocol. Section 5 concludes and discusses related and future work.

2 Preliminaries

Nondeterministic probabilistic labelled transition systems (pLTSs) [33] represent a very general semantic model for probabilistic processes as they combine LTSs [26] and discrete time Markov chains [34, 23], to model reactive behaviour, nondeterminism and probability. The state space is given by a *signature* Σ consisting of both a set of *operators* and a *rank function* r, where $\mathsf{r}(f)$ returns the arity of the operator f. The set $\mathsf{T}(\Sigma)$ of *terms* over Σ, or *processes*, is the least set such that $f(t_1, \ldots, t_n) \in \mathsf{T}(\Sigma)$ whenever $f \in \Sigma$, $\mathsf{r}(f) = n$ and $t_1, \ldots, t_n \in \mathsf{T}(\Sigma)$. Notice that $\mathsf{T}(\Sigma) \neq \emptyset$ if and only if Σ contains *constants*, i.e., functions with arity 0. We write $\Delta(\mathsf{T}(\Sigma))$ to denote the set of all probability distributions with *finite support* over $\mathsf{T}(\Sigma)$, which are mappings $\pi \colon \mathsf{T}(\Sigma) \to [0, 1]$, with $\sum_{t \in \mathsf{T}(\Sigma)} \pi(t) = 1$.

▶ **Definition 1** (pLTS [33]). A *nondeterministic probabilistic labelled transition system* (*pLTS*) is given by a triple $P = (\mathsf{T}(\Sigma), \mathit{Act}, \to)$ where:

(i) Σ is a signature,
(ii) Act is a countable set of *actions*, and
(iii) $\to \subseteq \mathsf{T}(\Sigma) \times \mathit{Act} \times \Delta(\mathsf{T}(\Sigma))$ is a *transition relation*.

As usual, we write $t \xrightarrow{\alpha} \pi$ for $(t, \alpha, \pi) \in \rightarrow$. Let $der(t, \alpha) = \{\pi \in \Delta(\mathsf{T}(\Sigma)) \mid t \xrightarrow{\alpha} \pi\}$ be the set of the *derivatives* of t according to action α. We say that a pLTS P is *image finite* if $der(t, \alpha)$ is finite for all $t \in \mathsf{T}(\Sigma)$ and $\alpha \in Act$.

We consider a signature that contains many of the operators from probabilistic CCS and probabilistic CSP specified via the SOS rules in Table 1–3. The operators we consider are:

1. constants $\mathsf{0}$ (idle process) and ε (skip process);
2. a family of n-ary probabilistic prefix operators $\alpha.([p_1]\_ \oplus \ldots \oplus [p_n]\_)$ with $\alpha \in Act$, $n \geq 1$, $p_1, \ldots, p_n \in (0, 1]$ and $\sum_{i=1}^{n} p_i = 1$;
3. nondeterministic choice $\_ + \_$;
4. action restriction $(\nu\, \alpha)\_$ with $\alpha \in Act \setminus \{\tau, \surd\}$;
5. sequential composition $\_\,;\_$;
6. CSP-like parallel composition $\_ \parallel_B \_$, with $B \subseteq Act \setminus \{\tau, \surd\}$,
7. CCS-like parallel composition $\_ \mid \_$, which assumes a function $^-\colon Act \setminus \{\tau, \surd\} \rightarrow Act \setminus \{\tau, \surd\}$ with $\overline{\overline{a}} = a$,
8. probabilistic choice $\_ +_p \_$;
9. finite iteration $\_^n$,
10. finite replication $!^n\_$,
11. infinite iteration $\_^\omega$,
12. binary Kleene-star iteration $\_^*\_$,
13. infinite replication (bang) operator $!\_$, and
14. probabilistic bang operator $!_p\_$.

All rules in Table 1–3 obey to the *PGSOS format* [9, 10]. We assume a set of actions $Act = A \cup \{\tau, \surd\}$, with $\surd$ denoting the *successful* termination action, and τ denoting *non-observable* action. We let $\alpha, \beta, \ldots$ range over Act and $a, b, \ldots$ over $Act \setminus \{\tau\}$. The rules of Table 1–3 assume a set of *process variables*, ranged over by x, y and a set of *distribution variables*, ranged over by μ, ν, allowing us to generalise the notions of term and distribution to *open term* and *open distribution* in the standard way. The rules are then defined by using *open transitions*, such as $x \mid y \xrightarrow{a} \mu \mid \nu$, taking open terms to open distributions. The PGSOS rules rely on some notations and operations on distributions. For $t \in \mathsf{T}(\Sigma)$, $\delta(t)$ denotes the *Dirac distribution*, defined by $(\delta(t))(t) = 1$. The convex combination $\sum_{i\in I} p_i\pi_i$ of a finite set of distributions $\{\pi_i\}_{i\in I}$, 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 write $\pi \oplus_p \pi'$ for $p\pi + (1-p)\pi'$. For $f \in \Sigma$ and $\pi_i \in \Delta(\mathsf{T}(\Sigma))$, $f(\pi_1, \ldots, \pi_n)$ denotes the product distribution defined by $f(\pi_1, \ldots, \pi_n)(f(t_1, \ldots, t_n)) = \prod_{i=1}^{n} \pi_i(t_i)$. Notice that all distributions defined in this inductive way have *finite support*.

▶ **Definition 2** (PGSOS-TSS [6, 9]). A *PGSOS-transition system specification* (*PGSOS-TSS*) is a triple $T = (\Sigma, Act, R)$ where:

- **(i)** Σ is a signature,
- **(ii)** Act is a countable set of actions,
- **(iii)** R is a countable set of PGSOS rules,
- **(iv)** for each $f \in \Sigma$ and $\alpha \in Act$, the set of rules with conclusion of the form $f(x_1, \ldots, x_n) \xrightarrow{\alpha} \theta$ is finite.

We recall that *closed substitutions* map process variables to processes, and distribution variables to distributions. Closed substitutions allows us to derive the *supported model* of a TSS, namely a pLTS in which the transition relation $\rightarrow$ contains all and only those transitions inductively derived by the SOS rules [7, 6, 9]. Item (4) in Definition 2 ensures that the supported model of a TSS is always image finite.

▶ **Definition 3** (Disjoint extension [1]). Let $T_1 = (\Sigma_1, A, R_1)$ and $T_2 = (\Sigma_2, A, R_2)$ be two PGSOS-TSSs. We say that T_2 is a *disjoint extension* of T_1, written $T_1 \sqsubseteq T_2$, iff $\Sigma_1 \subseteq \Sigma_2$, $R_1 \subseteq R_2$ and R_2 introduces no new rule for any operator in Σ_1.

2.1 Weak behavioural distances

In this section, we give the formal definitions of the weak behavioural distances of [18, 30].

The definition of weak transitions $\stackrel{\alpha}{\Longrightarrow}$, which abstract away non-observable actions, is complicated by the fact that transitions take processes to distributions. Following [16], we need to generalise transitions, so that they take sub-distributions to sub-distributions. With an abuse of notation, we use π, π' to range also over sub-distributions, admitting $\sum_{t \in \mathsf{T}(\Sigma)} \pi(t) \leq 1$. For a term t and a distribution π, we write $t \xrightarrow{\hat{\tau}} \pi$ if $t \xrightarrow{\tau} \pi$ or $\pi = \delta(t)$. Then, for $a \in A$, we write $t \xrightarrow{\hat{a}} \pi$ if $t \xrightarrow{a} \pi$. Relation $\xrightarrow{\hat{\alpha}}$ is extended to model transitions from sub-distributions to sub-distributions. For a sub-distribution $\pi = \sum_{i \in I} p_i \delta(t_i)$, we write $\pi \xrightarrow{\hat{\alpha}} \pi'$ if there is a set $J \subseteq I$ with $t_j \xrightarrow{\hat{\alpha}} \pi_j$ for all $j \in J$, $t_i \not\xrightarrow{\hat{\alpha}}$, for all $i \in I \setminus J$, and $\pi' = \sum_{j \in J} p_j \pi_j$. If $\alpha \neq \tau$ then this definition entails that only some terms in the support of π have the $\xrightarrow{\hat{\alpha}}$ transition. Then, we define the weak transition relation $\stackrel{\hat{\tau}}{\Longrightarrow}$ as the transitive and reflexive closure of $\xrightarrow{\hat{\tau}}$, i.e. $\stackrel{\hat{\tau}}{\Longrightarrow} = (\xrightarrow{\hat{\tau}})^*$, while for $a \in A$ we let $\stackrel{\hat{a}}{\Longrightarrow}$ denote $\stackrel{\hat{\tau}}{\Longrightarrow}\xrightarrow{\hat{a}}\stackrel{\hat{\tau}}{\Longrightarrow}$.

Weak bisimilarity metric [18] (resp. weak similarity quasimetric [30]) is defined as a pseudometric (resp. pseudoquasimetric) measuring the tolerance of the probabilistic weak bisimilarity (resp. probabilistic weak similarity).

▶ **Definition 4** (Pseudoquasimetrics and pseudometrics). A function $d\colon \mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma) \to [0,1]$ is said to be a *1-bounded pseudoquasimetric* when:
(i) $d(t,t) = 0$, for all $t \in \mathsf{T}(\Sigma)$, and
(ii) $d(t,t') \leq d(t,t'') + d(t'',t')$, for all $t, t', t'' \in \mathsf{T}(\Sigma)$.
If it is also symmetric, i.e. $d(t,t') = d(t',t)$, for all $t, t' \in \mathsf{T}(\Sigma)$, then it is said to be a *1-bounded pseudometric*.

We need to lift these two definitions to (sub)distributions. To this end, as in [30], we rely on the notions of *matching* [37] (also known as *coupling*) and *Kantorovich lifting* [25]. The original formulation in [18] is technically different, but equivalent [15].

▶ **Definition 5** (Matching). A *matching* for a pair of distributions (π, π') is a distribution ω in the product space $\mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma)$ with $\sum_{t' \in \mathsf{T}(\Sigma)} \omega(t,t') = \pi(t)$, for $t \in \mathsf{T}(\Sigma)$, and $\sum_{t \in \mathsf{T}(\Sigma)} \omega(t,t') = \pi'(t')$, for $t' \in \mathsf{T}(\Sigma)$. Let $\Omega(\pi, \pi')$ be the set of all matchings for (π, π').

▶ **Definition 6** (Kantorovich lifting). Let $d\colon \mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma) \to [0,1]$ be a pseudo(quasi)metric. The *Kantorovich lifting* of d is the function $\mathbf{K}(d)\colon \Delta(\mathsf{T}(\Sigma)) \times \Delta(\mathsf{T}(\Sigma)) \to [0,1]$ defined as:

$$\mathbf{K}(d)(\pi, \pi') \;=\; \min_{\omega \in \Omega(\pi,\pi')} \sum_{t,t' \in \mathsf{T}(\Sigma)} \omega(t,t') \cdot d(t,t').$$

Note that since we are considering only distributions with finite support, the minimum over the set of matchings $\Omega(\pi, \pi')$ is well defined.

Now, we are ready to define our behavioural distances. They are parametric on a *discount factor* $\lambda \in (0,1]$ which mitigates the (bi)simulation tolerance on future activities [12, 17].

▶ **Definition 7** (Weak behavioural distances). Let $|\pi|$ be an abbreviation for $\sum_{t \in \mathsf{T}(\Sigma)} \pi(t)$. We say that a pseudoquasimetric $d\colon \mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma) \to [0,1]$ is a *weak simulation quasimetric* if for all $s, t \in \mathsf{T}(\Sigma)$, with $d(s,t) < 1$, whenever $s \xrightarrow{\alpha} \pi_s$ there is a sub-distribution π_t such that $t \stackrel{\hat{\alpha}}{\Longrightarrow} \pi_t$ and $\lambda \cdot \mathbf{K}(d)(\pi_s, \pi_t + (1 - |\pi_t|)\mathsf{0}) \leq d(s,t)$. Moreover, if d is a pseudometric, then d is a *weak bisimulation metric*.

In the previous definition, if $|\pi_t| < 1$ then, with probability $1 - |\pi_t|$, there is no way to simulate the behaviour of any process different from $\mathsf{0}$ in the support of π_s. We remark that the kernel of a weak bisimulation pseudometric is a weak probabilistic bisimulation [18] and the kernel of a weak simulation pseudoquasimetric is a weak probabilistic simulation [30].

Crucial results are the existence of both the minimal weak bisimulation metric [18], called *weak bisimilarity metric*, and denoted with $\mathbf{d}^{\mathsf{m}}$, and the minimal weak simulation quasimetric [30], called *weak similarity quasimetric*, and denoted with $\mathbf{d}^{\mathsf{q}}$.

3 Uniform continuity for rooted (quasi)metric semantics

In this section, we show that the operators in Table 1–3 allow for compositional reasoning with respect to a *rooted* variant of our weak behavioural distances. We start by recalling the notion of uniform continuity, whose intuitive meaning was discussed in the Introduction.

▶ **Definition 8** (Modulus of continuity)**.** Let $T = (\Sigma, Act, R)$ be a TSS, $f \in \Sigma$ an n-ary operator, and $d\colon \mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma) \to [0,1]$ a function. A mapping $\omega_f\colon [0,1]^n \to [0,1]$ is a *modulus of continuity* for f with respect to d when:

- $d(f(s_1,\ldots,s_n), f(t_1,\ldots,t_n)) \leq \omega_f(d(s_1,t_1),\ldots,d(s_n,t_n))$, for all processes $s_i, t_i \in \mathsf{T}(\Sigma)$;
- ω_f is continuous at $(0,\ldots,0)$, i.e. $\lim_{(\epsilon_1,\ldots,\epsilon_n)\to(0,\ldots,0)} \omega(\epsilon_1,\ldots,\epsilon_n) = \omega(0,\ldots,0)$;
- $\omega_f(0,\ldots,0) = 0$.

▶ **Definition 9** (Uniformly continuous operator [20])**.** Let $T = (\Sigma, A, R)$ be a TSS and $d\colon \mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma) \to [0,1]$. We say that an operator $f \in \Sigma$ is:

- *uniformly continuous with respect to d* if f admits some modulus of continuity wrt. d;
- *L-Lipschitz continuous with respect to d*, for $L \in \mathbb{R}_{\geq 1}$, if $\omega_f(\epsilon_1,\ldots,\epsilon_n) = L \cdot \sum_{i=1}^{n} \epsilon_i$ is a modulus of continuity for f with respect to d;
- *non-expansive with respect to d* if f is 1-Lipschitz continuous with respect to d;
- *non-extensive with respect to d* if $\omega_f(\epsilon_1,\ldots,\epsilon_n) = \max_{i=1}^{n} \epsilon_i$ is a modulus of continuity for f with respect to d.

As expected, since τ-transitions may solve nondeterminism, $\mathbf{d}^{\mathsf{m}}$ is not uniformly continuous with respect to $+$, thus requiring to introduce a rooted version for $\mathbf{d}^{\mathsf{m}}$. For instance, $\mathbf{d}^{\mathsf{m}}(\tau.a.\mathsf{0}, a.\mathsf{0}) = 0$ but $\mathbf{d}^{\mathsf{m}}(\tau.a.\mathsf{0} + b.\mathsf{0}, a.\mathsf{0} + b.\mathsf{0}) = \lambda$, thus implying that no modulus of continuity for operator $+$ with respect to $\mathbf{d}^{\mathsf{m}}$ can be defined. Interestingly, in the metric context also the asymmetric simulation-like approach requires rootedness. Indeed, $\mathbf{d}^{\mathsf{q}}$ is not continuous with respect to $+_p$. For instance, $\mathbf{d}^{\mathsf{q}}(\tau.a.b.\mathsf{0}, a.b.\mathsf{0}) = 0$, but $\mathbf{d}^{\mathsf{q}}(\tau.a.b.\mathsf{0} +_p a.\mathsf{0}, a.b.\mathsf{0} +_p a.\mathsf{0}) = \lambda^2(1-p)$, thus implying that no modulus of continuity for $+_p$ wrt. $\mathbf{d}^{\mathsf{q}}$ can be defined. In fact, transition $\tau.a.b.\mathsf{0} +_p a.\mathsf{0} \xrightarrow{\tau} \delta(a.b.\mathsf{0})$ can be simulated only by $a.b.\mathsf{0} +_p a.\mathsf{0} \stackrel{\tau}{\Longrightarrow} \delta(a.b.\mathsf{0} +_p a.\mathsf{0})$, then $\lambda\,\mathbf{K}(\mathbf{d}^{\mathsf{q}})(\delta(a.b.\mathsf{0}), \delta(a.b.\mathsf{0} +_p a.\mathsf{0})) = \lambda \mathbf{d}^{\mathsf{q}}(a.b.\mathsf{0}, a.b.\mathsf{0} +_p a.\mathsf{0}) = \lambda^2(1-p)$. Notice that we also have that $\mathbf{d}^{\mathsf{m}}(\tau.a.b.\mathsf{0}, a.b.\mathsf{0}) = 0$ and $\mathbf{d}^{\mathsf{m}}(\tau.a.b.\mathsf{0} +_p a.\mathsf{0}, a.b.\mathsf{0} +_p a.\mathsf{0}) \geq \lambda^2(1-p)$. This implies that $\mathbf{d}^{\mathsf{m}}$, like $\mathbf{d}^{\mathsf{q}}$, is not uniformly continuous with respect to $+_p$.

▶ **Definition 10** (Rooted behavioural distances)**.** We say that a pseudoquasimetric $r\colon \mathsf{T}(\Sigma) \times \mathsf{T}(\Sigma) \to [0,1]$ is a *rooted simulation quasimetric* if there exists a weak simulation quasimetric d such that for all $s, t \in \mathsf{T}(\Sigma)$, with $r(s,t) < 1$, whenever $s \xrightarrow{\alpha} \pi_s$ there is a distribution π_t such that $t \xrightarrow{\alpha} \pi_t$ and $\lambda \cdot \mathbf{K}(d)(\pi_s, \pi_t) \leq r(s,t)$. Moreover, if both r and d are pseudometrics, then r is a *rooted bisimulation metric*.

Table 1 Non-extensive operators

$$\frac{}{\varepsilon \xrightarrow{\checkmark} \delta(\mathsf{0})} \qquad \frac{}{\alpha.\bigoplus_{i=1}^{n}[p_i]x_i \xrightarrow{\alpha} \sum_{i=1}^{n} p_i\delta(x_i)} \qquad \frac{x \xrightarrow{\alpha} \mu}{x+y \xrightarrow{\alpha} \mu} \qquad \frac{y \xrightarrow{\alpha} \nu}{x+y \xrightarrow{\alpha} \nu}$$

$$\frac{x \xrightarrow{\alpha} \mu \quad y \not\xrightarrow{\alpha}}{x +_p y \xrightarrow{\alpha} \mu} \qquad \frac{x \not\xrightarrow{\alpha} \quad y \xrightarrow{\alpha} \nu}{x +_p y \xrightarrow{\alpha} \nu} \qquad \frac{x \xrightarrow{\alpha} \mu \quad y \xrightarrow{\alpha} \nu}{x +_p y \xrightarrow{\alpha} \mu \oplus_p \nu} \qquad \frac{x \xrightarrow{\alpha} \mu \text{ and } \alpha \notin \{\beta, \overline{\beta}\}}{(\nu\,\beta)\,x \xrightarrow{\alpha} \mu}$$

▶ **Theorem 11.** *There exists a rooted simulation quasimetric* $\mathbf{r}^{\mathsf{q}}$ *(resp. rooted bisimulation metric* $\mathbf{r}^{\mathsf{m}}$*) such that* $\mathbf{r}^{\mathsf{q}}(s,t) \leq r(s,t)$ *(resp.* $\mathbf{r}^{\mathsf{m}}(s,t) \leq r(s,t)$*) for all rooted simulation quasimetrics (resp. rooted bisimulation metrics)* r *and all processes* $s,t \in \mathcal{T}(\Sigma)$*.*

We call $\mathbf{r}^{\mathsf{q}}$ *rooted similarity quasimetric*, and $\mathbf{r}^{\mathsf{m}}$ *rooted bisimilarity metric.*

In the following, for each operator, we compute a suitable upper bound on the rooted simulation and bisimulation tolerance between processes composed by that operator, then we use this bound to infer its compositionality property. Basically, our goal is to express a bound on the rooted (bi)simulation tolerance between composed processes $f(s_1,\ldots,s_n)$ and $f(t_1,\ldots,t_n)$ in terms of the tolerance between the components s_i and t_i.

Non-extensive operators. Consider the TSS $T_{\mathrm{NExt}} = (\Sigma_{\mathrm{NExt}}, Act, R_{\mathrm{NExt}})$ given by the rules R_{NExt} in Table 1. We show that all operators in Table 1 are non-extensive.

▶ **Proposition 12.** *Assume any TSS* $T = (\Sigma, A, R)$ *with* $T_{NExt} \sqsubseteq T$ *and* $s_i, t_i \in \mathcal{T}(\Sigma)$*. For* $\mathsf{j} \in \{\mathsf{q},\mathsf{m}\}$*, let us define* $r^{\mathsf{j}}_{(s,t,t')} = \min(\mathbf{r}^{\mathsf{j}}(s,t), \mathbf{r}^{\mathsf{j}}(s,t'))$ *and* $r^{\mathsf{j}}_{(q,s,t,t')} = \min(\mathbf{r}^{\mathsf{j}}(s,t), q(\mathbf{r}^{\mathsf{j}}(s,t)) + (1-q)\mathbf{r}^{\mathsf{j}}(s,t'))$*. Then, we have:*

(a) $\mathbf{r}^{\mathsf{j}}(\alpha.\bigoplus_{i=1}^{n}[p_i]s_i, \alpha.\bigoplus_{i=1}^{n}[p_i]t_i) \leq \lambda \cdot \sum_{i=1}^{n} p_i \mathbf{r}^{\mathsf{j}}(s_i,t_i)$ *with* $\mathsf{j} \in \{\mathsf{q},\mathsf{m}\}$*;*
(b) $\mathbf{r}^{\mathsf{q}}(s_1+s_2, t_1+t_2) \leq \max(r^{\mathsf{q}}_{(s_1,t_1,t_2)}, r^{\mathsf{q}}_{(s_2,t_1,t_2)})$*;*
(c) $\mathbf{r}^{\mathsf{m}}(s_1+s_2, t_1+t_2) \leq \max(r^{\mathsf{m}}_{(s_1,t_1,t_2)}, r^{\mathsf{m}}_{(s_2,t_1,t_2)}, r^{\mathsf{m}}_{(t_1,s_1,s_2)}, r^{\mathsf{m}}_{(t_2,s_1,s_2)})$*;*
(d) $\mathbf{r}^{\mathsf{q}}(s_1 +_p s_2, t_1 +_p t_2) \leq \max(r^{\mathsf{q}}_{(p,s_1,t_1,t_2)}, r^{\mathsf{q}}_{((1-p),s_2,t_2,t_1)})$*;*
(e) $\mathbf{r}^{\mathsf{m}}(s_1 +_p s_2, t_1 +_p t_2) \leq \max(r^{\mathsf{m}}_{(p,s_1,t_1,t_2)}, r^{\mathsf{m}}_{((1-p),s_2,t_2,t_1)}), r^{\mathsf{m}}_{(p,t_1,s_1,s_2)}, r^{\mathsf{m}}_{((1-p),t_2,s_2,s_1)})$*;*
(f) $\mathbf{r}^{\mathsf{j}}((\nu\,\alpha)\,s, (\nu\,\alpha)\,t) \leq \mathbf{r}^{\mathsf{j}}(s,t)$ *with* $\mathsf{j} \in \{\mathsf{q},\mathsf{m}\}$*.*

As expected, the asymmetry leads to have upper bounds for $\mathbf{r}^{\mathsf{q}}$ below those for $\mathbf{r}^{\mathsf{m}}$. For instance, by Proposition 12.2 we get $\mathbf{r}^{\mathsf{q}}(a.\mathsf{0}+a.\mathsf{0}, a.\mathsf{0}+b.\mathsf{0}) \leq \max(\min(0,1),\min(0,1)) = 0$, while by Proposition 12.3 $\mathbf{r}^{\mathsf{m}}(a.\mathsf{0}+a.\mathsf{0}, a.\mathsf{0}+b.\mathsf{0}) \leq \max(\min(0,1),\min(0,1),\min(0,0),\min(1,1)) = 1$.

Note that in Proposition 12 we have $T_{\mathrm{NExt}} \sqsubseteq T$ (Definition 3), namely processes s_i and t_i are obtained by using arbitrary operators, not necessarily only operators in Σ_{NExt}. Thus, these bounds hold independently from T. The following result follows from Proposition 12.

▶ **Theorem 13.** *The operators in Table 1 are non-extensive with respect to* $\mathbf{r}^{\mathsf{q}}$ *and* $\mathbf{r}^{\mathsf{m}}$*.*

Non-expansive operators. We proceed to show that all operators in Table 2 are non-expansive. Consider the TSS $T_{\mathrm{NExp}} = (\Sigma_{\mathrm{NExp}}, Act, R_{\mathrm{NExp}})$ with $T_{\mathrm{NExt}} \sqsubseteq T_{\mathrm{NExp}}$ and R_{NExp} containing the rules in Table 2, besides those in Table 1.

Table 2 Non-expansive operators, where the operator $|$ assumes a function $^- : Act \setminus \{\tau, \surd\} \to Act \setminus \{\tau, \surd\}$ with $\overline{\overline{a}} = a$, and the operator $||_B$ is defined for $B \subseteq Act \setminus \{\tau, \surd\}$

$$\frac{x \xrightarrow{\alpha} \mu}{x \mid y \xrightarrow{\alpha} \mu \mid \delta(y)} \qquad \frac{y \xrightarrow{\alpha} \nu}{x \mid y \xrightarrow{\alpha} \delta(x) \mid \nu} \qquad \frac{x \xrightarrow{a} \mu \quad y \xrightarrow{\overline{a}} \nu \quad a \in Act \setminus \{\tau, \surd\}}{x \mid y \xrightarrow{\tau} \mu \mid \nu}$$

$$\frac{x \xrightarrow{\surd} \mu \quad y \xrightarrow{\surd} \nu}{x \mid y \xrightarrow{\surd} \delta(0)} \qquad \frac{x \xrightarrow{\alpha} \mu \quad a \neq \surd}{x; y \xrightarrow{\alpha} \mu; \delta(y)} \qquad \frac{x \xrightarrow{\surd} \mu \quad y \xrightarrow{\alpha} \nu}{x; y \xrightarrow{\alpha} \nu} \qquad \frac{x \xrightarrow{\surd} \mu \quad y \xrightarrow{\surd} \nu}{x \mid\mid_B y \xrightarrow{\surd} \delta(0)}$$

$$\frac{x \xrightarrow{a} \mu \quad y \xrightarrow{a} \nu \quad a \in B}{x \mid\mid_B y \xrightarrow{a} \mu \mid\mid_B \nu} \qquad \frac{x \xrightarrow{\alpha} \mu \quad \alpha \notin (B \cup \{\surd\})}{x \mid\mid_B y \xrightarrow{\alpha} \mu \mid\mid_B \delta(y)} \qquad \frac{y \xrightarrow{\alpha} \nu \quad \alpha \notin (B \cup \{\surd\})}{x \mid\mid_B y \xrightarrow{\alpha} \delta(x) \mid\mid_B \nu}$$

▶ **Proposition 14.** *Assume any TSS $T = (\Sigma, A, R)$ with $T_{NExp} \sqsubseteq T$ and $s_i, t_i \in \mathcal{T}(\Sigma)$. For $\mathsf{j} \in \{\mathsf{q}, \mathsf{m}\}$ we have:*

(a) $\mathbf{r}^{\mathsf{j}}(s_1; s_2, t_1; t_2) \leq \begin{cases} 1 & \text{if } \mathbf{r}^{\mathsf{j}}(s_1, t_1)=1 \\ \max\{\mathbf{r}^{\mathsf{j}}(s_1, t_1)+\lambda(1-\frac{\mathbf{r}^{\mathsf{j}}(s_1,t_1)}{\lambda})\mathbf{r}^{\mathsf{j}}(s_2, t_2)\,,\ \mathbf{r}^{\mathsf{j}}(s_2, t_2)\} & \text{if } \mathbf{r}^{\mathsf{j}}(s_1, t_1)\in[0, 1) \end{cases}$

(b) $\mathbf{r}^{\mathsf{j}}(s_1 \mid s_2, t_1 \mid t_2) \leq r^{\mathsf{j}}_{\mathsf{synch}}$

(c) $\mathbf{r}^{\mathsf{j}}(s_1 \parallel_B s_2, t_1 \parallel_B t_2) \leq \begin{cases} r^{\mathsf{j}}_{\mathsf{synch}} & \text{if } B \neq \emptyset \\ r^{\mathsf{j}}_{\mathsf{asynch}} & \text{otherwise} \end{cases}$

with

$$r^{\mathsf{j}}_{\mathsf{synch}} = \begin{cases} 1 & \text{if } \mathbf{r}^{\mathsf{j}}(s_1, t_1) = 1 \vee \mathbf{r}^{\mathsf{j}}(s_2, t_2) = 1 \\ \mathbf{r}^{\mathsf{j}}(s_1, t_1) + \mathbf{r}^{\mathsf{j}}(s_2, t_2) - \frac{\mathbf{r}^{\mathsf{j}}(s_1,t_1)\mathbf{r}^{\mathsf{j}}(s_2,t_2)}{\lambda} & \text{otherwise} \end{cases}$$

$$r^{\mathsf{j}}_{\mathsf{asynch}} = \begin{cases} 1 & \text{if } \mathbf{r}^{\mathsf{j}}(s_1, t_1)=1 \vee \mathbf{r}^{\mathsf{j}}(s_2, t_2)=1 \\ \max\{\mathbf{r}^{\mathsf{j}}(s_1, t_1) + \lambda^2\mathbf{r}^{\mathsf{j}}(s_2, t_2) - \lambda\mathbf{r}^{\mathsf{j}}(s_1, t_1)\mathbf{r}^{\mathsf{j}}(s_2, t_2), & \\ \quad \mathbf{r}^{\mathsf{j}}(s_2, t_2) + \lambda^2\mathbf{r}^{\mathsf{j}}(s_1, t_1) - \lambda\mathbf{r}^{\mathsf{j}}(s_1, t_1)\mathbf{r}^{\mathsf{j}}(s_2, t_2)\} & \text{otherwise.} \end{cases}$$

Let us explain first Proposition 14.1. If $\mathbf{r}^{\mathsf{j}}(s_1, t_1) = 1$ then the maximal distance between s_1 and t_1 extends to $s_1; s_2$ and $t_1; t_2$. If $\mathbf{r}^{\mathsf{j}}(s_1, t_1) < 1$ then $\mathbf{r}^{\mathsf{j}}(s_1; s_2\,,\ t_1; t_2)$ is the maximum between the values given by the two different scenarios:

(i) the first one is that s_1 and t_1 evolve followed by s_2 and t_2, thus implying that we observe the distance $\mathbf{r}^{\mathsf{j}}(s_1, t_1)$ between s_1 and t_1 plus the distance $\mathbf{r}^{\mathsf{j}}(s_2, t_2)$ between s_2 and t_2, weighted by the likelihood that s_1 and t_1 exhibit the same behaviour, which is at most $(1 - \mathbf{r}^{\mathsf{j}}(s_1, t_1)/\lambda)$, and discounted by λ, since s_2 and t_2 are delayed by at least one step;

(ii) the second scenario is that s_1 and t_1 terminate immediately, so that we can observe only the distance $\mathbf{r}^{\mathsf{j}}(s_2, t_2)$ between s_2 and t_2, with no discount.

Consider now Proposition 14.2. If $\mathbf{r}^{\mathsf{j}}(s_1, t_1) = 1$ or $\mathbf{r}^{\mathsf{j}}(s_2, t_2) = 1$ then the upper bound is immediate. Otherwise, we obtain $\mathbf{r}^{\mathsf{j}}(s_1 \mid s_2, t_1 \mid t_2)$ by summing the distances $\mathbf{r}^{\mathsf{j}}(s_1, t_1)$ and $\mathbf{r}^{\mathsf{j}}(s_2, t_2)$ and, then, by subtracting $\frac{\mathbf{r}^{\mathsf{j}}(s_1,t_1)\mathbf{r}^{\mathsf{j}}(s_2,t_2)}{\lambda}$, which allows us to weight one of the two distances, say $\mathbf{r}^{\mathsf{j}}(s_2, t_2)$ by the likelihood that the other two processes exhibit the same behaviour, namely $(1 - \frac{\mathbf{r}^{\mathsf{j}}(s_1,t_1)}{\lambda})$. Finally, consider Proposition 14.3. If processes can synchronise, then the upper bound is the same as Proposition 14.2. Otherwise, either s_1 and t_1 evolve and s_2 and t_2 are delayed, or, symmetrically, s_2 and t_2 evolve and s_1 and t_1 are delayed. The distance between the delayed processes is therefore discounted and we get a bound slightly below that of Proposition 14.2.

Table 3 Lipschitz continuous operators

$$\frac{x \xrightarrow{a} \mu \quad a \neq \surd}{x^{n+1} \xrightarrow{a} \mu;\delta(x^n)} \qquad \frac{x \xrightarrow{\surd} \mu}{x^{n+1} \xrightarrow{\surd} \mu} \qquad \frac{}{x^0 \xrightarrow{\surd} \delta(0)} \qquad \frac{x \xrightarrow{\surd} \mu \quad x \xrightarrow{a} \nu \quad a \neq \surd \quad n > m}{x^n \xrightarrow{a} \nu;\delta(x^m)}$$

$$\frac{x \xrightarrow{a} \mu \quad a \neq \surd}{!^{n+1}x \xrightarrow{a} \mu \,||_\emptyset\, \delta(!^n x)} \qquad \frac{x \xrightarrow{\surd} \mu}{!^{n+1}x \xrightarrow{\surd} \mu} \qquad \frac{}{!^0 x \xrightarrow{\surd} \delta(0)} \qquad \frac{x \xrightarrow{a} \mu \quad a \neq \surd}{x^\omega \xrightarrow{a} \mu;\delta(x^\omega)}$$

$$\frac{x \xrightarrow{a} \mu \quad a \neq \surd}{x^* y \xrightarrow{a} \mu;\delta(x^* y)} \qquad \frac{y \xrightarrow{a} \nu}{x^* y \xrightarrow{a} \nu} \qquad \frac{x \xrightarrow{a} \mu \quad a \neq \surd}{!x \xrightarrow{a} \mu \,|||\, \delta(!x)} \qquad \frac{x \xrightarrow{a} \mu \quad a \neq \surd}{!_p x \xrightarrow{a} \mu \oplus_p (\mu \,|||\, \delta(!_p x))}$$

Notice that also the processes s_i and t_i in Proposition 14 are obtained by using arbitrary operators, not necessarily in Σ_{NExp}. The following result follows from Proposition 14.

▶ **Theorem 15.** *The operators in Table 2 are non-expansive with respect to* $\mathbf{r}^{\mathsf{q}}$ *and* $\mathbf{r}^{\mathsf{m}}$.

Clearly, the results in Proposition 14 can be generalised to more complex terms. For instance, we give two generalizations of Proposition 14.2 that will be used in the case study presented in the next section.

▶ **Proposition 16.** *Assume processes* $s_1, t_1, \ldots, s_n, t_n$, *with* $n \geq 2$. *We have:*

$$\mathbf{r}^{\mathsf{m}}(s_1|\ldots|s_n, t_1|\ldots|t_n) \;\leq \sum_{\emptyset \subset I \subseteq \{1,\ldots,n\}} (-1)^{|I|+1} \prod_{i \in I} \mathbf{r}^{\mathsf{m}}(s_i, t_i) \;\; .$$

▶ **Proposition 17.** *Assume processes* $s_1, t_1, \ldots, s_n, t_n$, *with* $n \geq 2$. *If* $\mathbf{r}^{\mathsf{m}}(s_i, t_i) = r$ *for all* $i = 1, \ldots n$, *then we have:*

$$\mathbf{r}^{\mathsf{m}}(s_1|\ldots|s_n, t_1|\ldots|t_n) \;\leq\; -\sum_{i=1}^{n} \binom{n}{i} (-r)^i \;\; .$$

Lipschitz continuous operators. Now we show that all operators in Table 3 are Lipschitz continuous. Consider the TSS $T_{\mathrm{LC}} = (\Sigma_{\mathrm{LC}}, Act, R_{\mathrm{LC}})$ with $T_{\mathrm{NExp}} \sqsubseteq T_{\mathrm{LC}}$ and R_{LC} containing the rules in Table 3, besides those in Table 1–2.

▶ **Proposition 18.** *Assume any TSS* $T = (\Sigma, A, R)$ *with* $T_{LC} \sqsubseteq T$ *and* $s, s_i, t, t_i \in \mathcal{T}(\Sigma)$. *For* $\mathsf{j} \in \{\mathsf{q}, \mathsf{m}\}$ *we have:*

(a) $\mathbf{r}^{\mathsf{j}}(s^n, t^n) \leq \begin{cases} \mathbf{r}^{\mathsf{j}}(s,t)\frac{1-(\lambda-\mathbf{r}^{\mathsf{j}}(s,t))^n}{1-(\lambda-\mathbf{r}^{\mathsf{j}}(s,t))} & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in (0,1) \\ \mathbf{r}^{\mathsf{j}}(s,t) & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in \{0,1\} \end{cases}$

(b) $\mathbf{r}^{\mathsf{j}}(!^n s, !^n t) \leq \begin{cases} \mathbf{r}^{\mathsf{j}}(s,t)\frac{1-(\lambda^2-\lambda\mathbf{r}^{\mathsf{j}}(s,t))^n}{1-(\lambda^2-\lambda\mathbf{r}^{\mathsf{j}}(s,t))} & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in (0,1) \\ \mathbf{r}^{\mathsf{j}}(s,t) & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in \{0,1\} \end{cases}$

(c) $\mathbf{r}^{\mathsf{j}}(s^\omega, t^\omega) \leq \begin{cases} \mathbf{r}^{\mathsf{j}}(s,t)\frac{1}{1-(\lambda-\mathbf{r}^{\mathsf{j}}(s,t))} & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in (0,1) \\ \mathbf{r}^{\mathsf{j}}(s,t) & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in \{0,1\} \end{cases}$

(d) $\mathbf{r}^{\mathsf{j}}(!s, !t) \leq \begin{cases} \mathbf{r}^{\mathsf{j}}(s,t)\frac{1}{1-(\lambda^2-\lambda\mathbf{r}^{\mathsf{j}}(s,t))} & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in (0,1) \\ \mathbf{r}^{\mathsf{j}}(s,t) & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in \{0,1\} \end{cases}$

(e) $\mathbf{r}^{\mathsf{j}}(s_1{}^* s_2, t_1{}^* t_2) \leq \max(\mathbf{r}^{\mathsf{j}}(s_1{}^\omega, t_1{}^\omega), \mathbf{r}^{\mathsf{j}}(s_2, t_2))$

(f) $\mathbf{r}^{\mathsf{j}}(!_p s, !_p t) \leq \begin{cases} \mathbf{r}^{\mathsf{j}}(s,t)\frac{1}{1-(1-p)(\lambda^2-\lambda\mathbf{r}^{\mathsf{j}}(s,t))} & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in (0,1) \\ \mathbf{r}^{\mathsf{j}}(s,t) & \text{if } \mathbf{r}^{\mathsf{j}}(s,t) \in \{0,1\}. \end{cases}$

The bound in Proposition 18.1 is obtained by applying $n-1$ times the bound in Proposition 14 for operator $\_\,;\_$, the rationale being that the pLTS associated to s^n is isomorphic to that of process $s;\ldots;s$ with n occurrences of s. Similarly, the bound in Proposition 18.2 is obtained by applying $n-1$ times the bound in Proposition 14 for operator $\_\,||_\emptyset\,\_$, the rationale being that $!^n s$ denotes a pLTS isomorphic to that of process $s\,||_\emptyset \ldots ||_\emptyset\, s$ with n occurrences of s. The bounds in Proposition 18.3 and Proposition 18.4 are obtained by taking the limits for the bounds in Proposition 18.1 and Proposition 18.2, respectively. Proposition 18.5 is obtained by observing that the (bi)simulation tolerance between processes ${s_1}^* s_2$ and ${t_1}^* t_2$ is less than or equal to the maximum of the tolerance bound $\mathbf{r}^{\mathsf{j}}({s_1}^\omega, {t_1}^\omega)$ (infinite iteration of s_1 and t_1 such that s_2 and t_2 never evolve), and the tolerance bound $\mathbf{r}^{\mathsf{j}}(s_2,t_2)$ (s_2 and t_2 evolve immediately). The case where s_1 and t_1 iterate n-times and then s_2 and t_2 evolve leads always to a tolerance bound $\mathbf{r}^{\mathsf{j}}({s_1}^n,{t_1}^n) + (\lambda - \mathbf{r}^{\mathsf{j}}(s_1,t_1))^n \mathbf{r}^{\mathsf{j}}(s_2,t_2) \leq \max(\mathbf{r}^{\mathsf{j}}({s_1}^\omega,{t_1}^\omega), \mathbf{r}^{\mathsf{j}}(s_2,t_2))$. Finally, Proposition 18.6 can be understood by observing that $!_p s$ behaves as $!^{n+1}s$ with probability $p(1-p)^n$. Hence, by Proposition 18.2 we get $\mathbf{r}^{\mathsf{j}}(!_p s, !_p t) \leq \sum_{n=0}^{\infty} p(1-p)^n \mathbf{r}^{\mathsf{j}}(!^{n+1}s, !^{n+1}t) \leq \sum_{n=0}^{\infty} p(1-p)^n r^{\mathsf{j}}_{!^{n+1}} = \mathbf{r}^{\mathsf{j}}(s,t)/(1-(1-p)(\lambda^2 - \lambda \mathbf{r}^{\mathsf{j}}(s,t)))$.

Notice also that the processes s, t, s_i, t_i in Proposition 18 are obtained by using arbitrary operators, not necessarily in Σ_{LC}. The following result follows from Proposition 18.

▶ **Theorem 19.** *The operators*

(i) *finite iteration* $\_^n$
(ii) *finite replication* $!^n\_$
(iii) *probabilistic replication* $!_p\_$

are Lipschitz continuous with respect to $\mathbf{r}^{\mathsf{q}}$ *and* $\mathbf{r}^{\mathsf{m}}$ *for any* $\lambda \in (0,1]$. *The operators*

(i) *infinite iteration* $\_^\omega$
(ii) *nondeterministic Kleene-star iteration* $\_^*\_$
(iii) *infinite replication* $!\_$

are Lipschitz continuous with respect to $\mathbf{r}^{\mathsf{q}}$ *and* $\mathbf{r}^{\mathsf{m}}$ *for any* $\lambda \in (0,1)$.

Notice that discounting the distance observed at step n by λ^n is necessary to have compositionality of the operators $\_^\omega$, $\_^*\_$, and $!\_$.

4 A case study: Group Key Update

A *group key* is a secret key shared by a group of principals to secure their *multicast communications*. Group key update protocols were originally adopted to secure LANs [32]. Nowadays they are widely used in different contexts, such as: audio and video conferencing in Computer Supported Co-operative Work (CSCW), Virtual Private Networks (VPN), distributed databases, instant messaging applications, etc.

A crucial problem when dealing with key-secured communications is *rekeying*, i.e. the process of distributing new keys to the principals. Rekeying is necessary when a member joins the group, to prevent it to access the information exchanged in the past (*backward confidentiality*), and when a member leaves the group, to prevent it to access future data (*forward confidentiality*). Rekeying is managed either by a third trusted party or by a member acting as *group owner*. In our example, we abstract from these two solutions by assuming a unique *key manager entity* which takes care of rekeying.

We assume a set $\mathcal{N}$ of member IDs. For each members $i \in \mathcal{N}$, the probabilities of leaving and joining the group are $l(i)$ and $j(i)$, respectively. Furthermore, each member can leave/join the group at most n times. Notice that high values of n, $l(i)$ or $j(i)$ cause frequent rekeying, with obvious consequences on:

Table 4 An abstract group key update protocol.

$$
\begin{array}{lcl}
\mathit{Group}(l,j) & = & (\nu\,(\mathit{Act} \setminus \mathsf{newK}))\,\big(\mathit{Manager} \mid \prod_{i\in\mathcal{N}} \mathit{Member}(i,l(i),j(i))\big) \\
\mathit{Manager} & = & \mathit{Connected} \mid \big(\sum_{I\subseteq\mathcal{N}} \mathsf{act}_I; \mathit{Mng}(I)\big)^{\omega} \\
\mathit{Connected} & = & \overline{\mathsf{act}}_{\mathcal{N}}; \Big(\sum_{I\subseteq\mathcal{N}} \mathsf{sync}_I; \overline{\mathsf{act}}_I; \varepsilon\Big)^{\omega} \\
\mathit{Mng}(I) & = & \big(\sum_{i\in I} \mathsf{leave}_i; \overline{\mathsf{newK}}; \mathit{SendNewKey}(I\setminus i); \overline{\mathsf{sync}}_{I\setminus i}; \varepsilon\big) + \\
 & & \big(\sum_{i\in(\mathcal{N}\setminus I)} \mathsf{join}_i; \overline{\mathsf{newK}}; \mathit{SendNewKey}(I\cup i); \overline{\mathsf{sync}}_{I\cup i}; \varepsilon\big) \\
\mathit{SendNewKey}(\{i_1,\ldots,i_k\}) & = & \overline{(\mathsf{i}_1,\mathsf{Key})}; \ldots; \overline{(\mathsf{i}_k,\mathsf{Key})}; \varepsilon \\
\mathit{Member}(i,p,q) & = & \mathit{State}(i) \mid \big(\mathit{MembIn}(i,p) + \mathit{MembOut}(i,q)\big)^{n} \\
\mathit{State}(i) & = & \overline{\mathsf{in}}_i; \big(\overline{\mathsf{in}}_i{}^{*}; \mathsf{change}_i; \overline{\mathsf{out}}_i{}^{*}; \mathsf{change}_i; \varepsilon\big)^{*} \\
\mathit{MembIn}(i,p) & = & \mathsf{in}_i; \big((\mathsf{i},\mathsf{Key}) + \tau; \big((\overline{\mathsf{leave}}_i; \overline{\mathsf{change}}_i; \varepsilon) \oplus_p \varepsilon\big)\big) \\
\mathit{MembOut}(i,q) & = & \mathsf{out}_i; \tau; \big((\overline{\mathsf{join}}_i; \overline{\mathsf{change}}_i; (\mathsf{i},\mathsf{Key}); \varepsilon) \oplus_q \varepsilon\big)
\end{array}
$$

(a) the number of attacks aiming at compromising the group key,
(b) degradation of communication service,
(c) battery consumption.

Thus, in the following, a group key protocol in which members never leave/join the group (i.e. $l(i) = j(i) = 0$, for any $i \in \mathcal{N}$) will be called *ideal*.

Our goal is to show that the theory developed in the previous section represents an effective instrument to estimate the distance between the ideal protocol and possible variations of the protocol obtained by playing with the parameters n, $l(i)$ and $j(i)$, for $i \in \mathcal{N}$.

Table 4 reports an abstract representation of the rekeying process in terms of our general process algebra. Since cryptographic details are not relevant for our purposes, we protect communications via the restriction operator $(\nu\,\alpha)\,\_$. We observe only the signal newK denoting the rekeying event. For simplicity, in the protocol, we will write $I \setminus i$ instead of $I \setminus \{i\}$, and $I \cup i$ instead of $I \cup \{i\}$.

The process $\mathit{Group}(l,j)$ represents a group, in its initial configuration, containing all members in $\mathcal{N}$, each of which can leave/enter the group at most n times. This process consists of the parallel composition of the process *Manager* together with a process for each member in $\mathcal{N}$. The process *Manager* has two parallel components: (a) the process *Connected*, which determines those members which are currently part of the group, and (b) a process that upon reception of a signal act_I, with $I \subseteq \mathcal{N}$, it behaves as $\mathit{Mng}(I)$, i.e. the process managing the group with members in the set I. Initially, all members join the group. Thus, *Connected* starts by activating the process $\mathit{Mng}(\mathcal{N})$. Then, whenever *Connected* receives a signal sync_I (from some $\mathit{Mng}(J)$) it activates $\mathit{Mng}(I)$ by sending the signal act_I. Notice that, in this case, there is a member i such that either $I = J \setminus \{i\}$, because i has left the group, or $I = J \cup \{i\}$, because i has joined the group.

The process $\mathit{Mng}(I)$ behaves as follows. Whenever it senses a signal leave_i (resp. join_i) denoting that a connected member $i \in I$ (resp. an unconnected member $i \in \mathcal{N} \setminus I$) is leaving (resp. joining) the group, it performs the following actions:

(i) it signals the generation of a new key,
(ii) it broadcasts the new key to all members in $J = I \setminus i$ (resp. $J = I \cup i$), namely the members of the new group,
(iii) it communicates to *Connected* the new set of current members in the group via a signal sync_J.

The process $Member(i,p,q)$ consists of the parallel composition of the process $State(i)$, which stores the state of member i, together with either the process $MembIn(i,p)$, which describes the behaviour of i when it is in the group, or the process $MembOut(i,q)$, which describes the behaviour of i when it is out of the group. The signal in_i (resp. out_i) is used by $State(i)$ to activate $MembIn(i,p)$ (resp. $MembOut(i,q)$). Via process $MembIn(i,p)$, the member i may either receive the new key from the manager or leave the group with a probability p. Similarly, via process $MembOut(i,q)$, the member i may decide to join the group with probability q. If i succeeds in joining the group then a new group key is sent to i and all current members of the group. This completes the explanation of the protocol.

Now, let $\mathbf{p}$ denote the constant function $\mathbf{p}\colon \mathcal{N} \to [0,1]$, with $\mathbf{p}(i) = p$ for all $i \in \mathcal{N}$. Similarly, we define $\mathbf{q}$. Thus, $Group(\mathbf{p},\mathbf{q})$ denotes the instance of the protocol where all members have the same leave/join probability, whereas $Group(\mathbf{0},\mathbf{0})$ denotes the *ideal* group, where rekeying never occurs as the no principal leaves or join the group.

We start our analysis by providing an upper bound of the distance between the behaviours of an arbitrary member $i \in \mathcal{N}$, when varying leave/join probabilities. For that we need a technical lemma to estimate the distance between two occurrences of probabilistic prefix dealing with the same processes, but different probabilities.

▶ **Lemma 20.** *For all $s,t \in \mathcal{T}(\Sigma)$ we have $\mathbf{r}^{\mathsf{m}}(a.(s \oplus_p t), a.(s \oplus_q t)) \leq |p-q|$.*

▶ **Proposition 21.** *Let $p,q,p',q' \in [0,1]$, then*

$$\mathbf{r}^{\mathsf{m}}(Member(i,p,q), Member(i,p',q')) \;\leq\; \max(|p-p'|,|q-q'|)\frac{1-(1-r)^n}{1+r}.$$

Proof. By Lemma 20 and compositionality results in Proposition 12.1 and Prop. 12.2 we get $\mathbf{r}^{\mathsf{m}}(MembIn(i,p), MembIn(i,p')) \leq |p-p'|$ and $\mathbf{r}^{\mathsf{m}}(MembOut(i,q), MembOut(i,q')) \leq |q-q'|$. Then, the thesis follows by applying the compositionality results in Proposition 12.3, Proposition 14.2, Proposition 18.1 ◀

We can generalise this result by taking into account all members in $\mathcal{N}$.

▶ **Proposition 22.** *Given arbitrary functions $l,j,l',j'\colon \mathcal{N} \to [0,1]$, we have:*

$$\mathbf{r}^{\mathsf{m}}(Group(l,j), Group(l',j')) \leq \sum_{I\subseteq\mathcal{N}, I\neq\emptyset} (-1)^{|I|+1} \prod_{i\in I} r(i)\frac{1-(1-r(i))^n}{1+r(i)}$$

with $r(i) = \max(|l(i)-l'(i)|, |j(i)-j'(i)|)$.

Proof. By Proposition 21, Proposition 16 and the compositionality results of Proposition 14.2 and Proposition 12.6. ◀

Proposition 22 estimates the distance between an arbitrary group and the ideal one.

▶ **Corollary 23.** *For any $l,j,r\colon \mathcal{N} \to [0,1]$ such that $r(i) = \max(l(i),j(i))$, we have:*

$$\mathbf{r}^{\mathsf{m}}(Group(\mathbf{0},\mathbf{0}), Group(l,j)) \;\leq\; \sum_{I\subseteq\mathcal{N}, I\neq\emptyset} (-1)^{|I|+1} \prod_{i\in I} r(i)\frac{1-(1-r(i))^n}{1+r(i)} \quad .$$

We can also compare two instances of the protocol when assuming homogeneous probabilities (i.e. all members leaves/join the group with the same probabilities.)

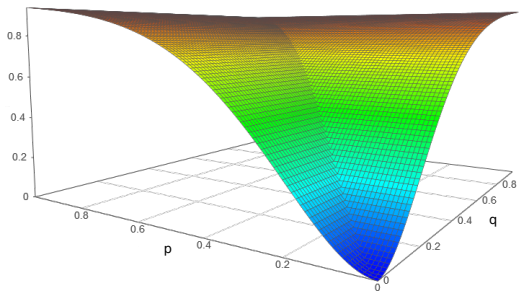

Figure 1 Upper bound to $\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{0},\mathbf{0}), \mathit{Group}(\mathbf{p},\mathbf{q}))$

▶ **Proposition 24.** *For arbitrary probabilities $p, p', q, q' \in [0,1]$ we have:*

$$\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{p},\mathbf{q}), \mathit{Group}(\mathbf{p}',\mathbf{q}')) \leq -\sum_{i=1}^{|\mathcal{N}|} \binom{|\mathcal{N}|}{i} \left(-r\frac{1-(1-r)^n}{1+r}\right)^i$$

with $r = \max(|p-p'|, |q-q'|)$.

Proof. By Proposition 21, Proposition 17 and the compositionality results of Proposition 12.6 and Proposition 14.2. ◀

This allows us to compare a group with homogeneous probabilities with the ideal group.

▶ **Corollary 25.** *For arbitrary probabilities $p, q \in [0,1]$ we have:*

$$\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{0},\mathbf{0}), \mathit{Group}(\mathbf{p},\mathbf{q})) \leq -\sum_{i=1}^{|\mathcal{N}|} \binom{|\mathcal{N}|}{i} \left(-(\max(p,q)\frac{1-(1-(\max(p,q))^n}{1+(\max(p,q)}\right)^i.$$

For instance, assume an instance of the protocol with $\mathcal{N} = \{1,\ldots,4\}$ and $n = 3$. Then we have $\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{0},\mathbf{0}), \mathit{Group}(\mathbf{p},\mathbf{q})) \leq 4r - 6r^2 + 4r^3 - r^4$, with $r = \max(p,q)\frac{1-(1-\max(p,q))^3}{1+\max(p,q)}$. The upper bound is reported in Fig. 1. Notice that the surface is symmetric, meaning that the upper bounds for $p \geq q$ and $q \geq p$ coincide (because they depend on $\max(p,q)$).

Figures 2 and 3 describe the evolution of the upper bound of $\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{0},\mathbf{0}), \mathit{Group}(\mathbf{p},\mathbf{p}))$, i.e. when leave and join probability are the same ($p = q$). In Figure 2 we fix 4 members and we vary n in the set $\{3,5,7,9,11\}$. We can observe that $\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{0},\mathbf{0}), \mathit{Group}(\mathbf{p},\mathbf{p}))$ grows with n, in particular for group with low values of p and q. In Figure 3, we fix n equals to 3 and vary the number of members in the set $\{4,5,6,7,8\}$. We can observe that $\mathbf{r}^{\mathsf{m}}(\mathit{Group}(\mathbf{0},\mathbf{0}), \mathit{Group}(\mathbf{p},\mathbf{p}))$ grows with the size of the group, in particular in group with high values of p (and q).

Summarising, we can assert that the protocol under analysis has good efficiency in groups with low dynamicity, regardless of the size of the group.

5 Conclusions, related and future work

We showed that uniform continuity is an effective property to achieve compositional reasoning with respect to rooted (quasi)metric semantics. We considered all standard operators of

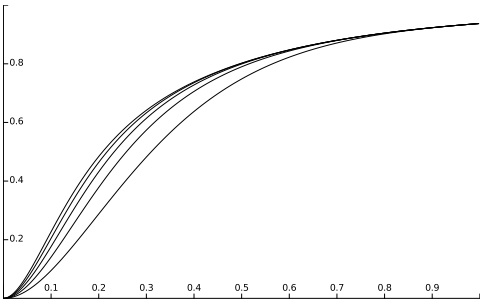

Figure 2 4 members and $n \in \{3, 5, 7, 9, 11\}$.

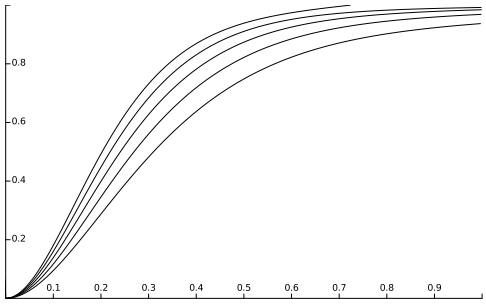

Figure 3 $n = 3$ and $4 \leq$ members ≤ 8.

probabilistic process algebra and provided suitable upper bounds on the distance between processes composed by these operators. This allows us to infer their uniform continuity with respect to both rooted bisimilarity metric and rooted similarity quasimetric. Interestingly, the rootedness condition, introduced to deal with nondeterministic and probabilistic choice, is crucial when dealing with similarity quasimetric. We exemplified how these semantic theories can be used to pursue compositional reasoning over a non-trivial protocol.

The current paper is the ideal continuation of [20]. In that paper, the authors show that uniform continuity captures the essential intuition of compositional reasoning when dealing with probabilistic processes. The proposal of [20] generalises and extends earlier proposals in [17, 2] to capture recursive operators. The focus of all these papers is on strong bisimulation metrics. We remark that, following [35, 17, 14], we have considered (bi)simulation-inspired (quasi)metric for the pLTS model. However, the literature offers also different approaches to estimate the distance between processes. In [19] a spectrum of distances between processes is obtained by applying the theory of quantitative Ehrenfeucht-Fraïssé games to transition systems. This theory allows to generate different notions of distance by means of different generalisations of a suitable distance over traces. Paper [11] studies distances between processes in the semantic model of Metric Transition Systems. In [3, 8] trace metrics for the model of Markov Chains are defined as total variation distances on the cones generated by the execution traces. In [29] the distance between systems is defined by means of a probabilistic approximated bisimulation. This paper provides a technique to compute upper bounds based on compositional algebraic laws.

As *future work*, we will extend the analysis of concrete process algebra operators to general SOS rule and specification formats. A SOS rule and specification format ensuring uniform continuity of operators with respect to strong bisimilarity metric has been proposed in [21, 22], the idea being that process arguments of operators are copied only finitely many times along their evolution. In order to achieve the same result in the weak case, it is necessary to strengthen the format of [21] by preventing that process replication can arise by τ-transitions. After that, we intend to extend our approach to the weak versions of other notions of distance, such as convex bisimulation metric [13], trace metric [19], and total-variation distance based metrics [31]. Finally, another possible research direction is develop a timed-variant of our technique to deal with timed aspects of systems as in [27, 28].

Acknowledgements. We thank the anonymous reviewers for valuable comments.

References

1 Luca Aceto, Bard Bloom, and Fritz W. Vaandrager. Turning SOS Rules into Equations. *Information & Computation*, 111(1):1–52, 1994. doi:10.1006/inco.1994.1040.

2 Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, and Radu Mardare. Computing Behavioral Distances, Compositionally. In *38th International Symposium on Mathematical Foundations of Computer Science*, volume 8087 of *LNCS*, pages 74–85. Springer, 2013. doi:10.1007/978-3-642-40313-2_9.

3 Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, and Radu Mardare. Converging from Branching to Linear Metrics on Markov Chains. In *12th International Colloquium on Theoretical Aspects of Computing*, volume 9399 of *LNCS*, pages 349–367. Springer, 2015. doi:10.1007/978-3-319-25150-9_21.

4 Christel Baier, Holger Hermanns, and Joost-Pieter Katoen. Probabilistic Weak Simulation is Decidable in Polynomial Time. *Information Processing Letters*, 89(3):123–130, 2004. doi:10.1016/j.ipl.2003.10.001.

5 Christel Baier, Joost-Pieter Katoen, Holger Hermanns, and Boudewijn R. Haverkort. Simulation for Continuous-Time Markov Chains. In *13th International Conf. on Concurrency Theory*, volume 2421 of *LNCS*, pages 338–354, 2002. doi:10.1007/3-540-45694-5_23.

6 Falk Bartels. *On Generalised Coinduction and Probabilistic Specification Formats.* PhD thesis, VU University Amsterdam, 2004.

7 Bard Bloom, Sorin Istrail, and Albert R. Meyer. Bisimulation Can't Be Traced. *Journal of the ACM*, 42:232–268, 1995. doi:10.1145/200836.200876.

8 Przemyslaw Daca, Thomas A. Henzinger, Jan Kretínský, and Tatjana Petrov. Linear Distances between Markov Chains. In *27th International Conference on Concurrency Theory*, LIPIcs, pages 20:1–20:15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.CONCUR.2016.20.

9 Pedro R. D'Argenio, Daniel Gebler, and Matias D. Lee. Axiomatizing Bisimulation Equivalences and Metrics from Probabilistic SOS Rules. In *17th International Conference on Foundations of Software Science and Computation Structures*, volume 8412 of *LNCS*, pages 289–303. Springer, 2014. doi:10.1007/978-3-642-54830-7_19.

10 Pedro R. D'Argenio, Daniel Gebler, and Matias D. Lee. A General SOS Theory for the Specification of Probabilistic Transition Systems. *Information & Computation*, 249:76–109, 2016. doi:10.1016/j.ic.2016.03.009.

11 Luca de Alfaro, Marco Faella, and Mariëlle Stoelinga. Linear and Branching System Metrics. *IEEE Trans. Software Eng.*, 35(2):258–273, 2009. doi:10.1109/TSE.2008.106.

12 Luca de Alfaro, Thomas A. Henzinger, and Rupak Majumdar. Discounting the Future in Systems Theory. In *30th Int. Colloquium on Automata, Languages and Programming*, volume 2719 of *LNCS*, pages 1022–1037. Springer, 2003. doi:10.1007/3-540-45061-0_79.

13 Luca de Alfaro, Rupak Majumdar, Vishwanath Raman, and Mariëlle Stoelinga. Game Relations and Metrics. In *22nd IEEE Symposium on Logic in Computer Science*, pages 99–108. IEEE Computer Society, 2007. doi:10.1109/LICS.2007.22.

14 Yuxin Deng, Tom Chothia, Catuscia Palamidessi, and Jun Pang. Metrics for Action-labelled Quantitative Transition Systems. *ENTCS*, 153(2):79–96, 2006. doi:10.1016/j.entcs.2005.10.033.

15 Yuxin Deng and Wenjie Du. The Kantorovich Metric in Computer Science: A Brief Survey. *ENTCS*, 253(3):73–82, 2009. doi:10.1016/j.entcs.2009.10.006.

16 Yuxin Deng, Rob J. van Glabbeek, Matthew Hennessy, and Carroll Morgan. Characterising Testing Preorders for Finite Probabilistic Processes. *Logical Methods in Computer Science*, 4(4), 2008. doi:10.2168/LMCS-4(4:4)2008.

17 Josée Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for Labelled Markov Processes. *Theoretical Computer Science*, 318(3):323–354, 2004. doi:10.1016/j.tcs.2003.09.013.

18 Josée Desharnais, Radha Jagadeesan, Vineet Gupta, and Prakash Panangaden. The Metric Analogue of Weak Bisimulation for Probabilistic Processes. In *17th IEEE Symposium on Logic in Computer Science*, pages 413–422. IEEE Computer Society, 2002. doi:10.1109/LICS.2002.1029849.

19 Uli Fahrenberg and Axel Legay. The Quantitative Linear-time-branching-time Spectrum. *Theoretical Computer Science*, 538:54–69, 2014. doi:10.1016/j.tcs.2013.07.030.

20 Daniel Gebler, Kim G. Larsen, and Simone Tini. Compositional Bisimulation Metric Reasoning with Probabilistic Process Calculi. *Logical Methods in Computer Science*, 12(4), 2016. doi:10.2168/LMCS-12(4:12)2016.

21 Daniel Gebler and Simone Tini. Fixed-point Characterization of Compositionality Properties of Probabilistic Processes Combinators. In *Combined 21th International Workshop on Expressiveness in Concurrency and 11th Workshop on Structural Operational Semantics*, volume 160 of *EPTCS*, pages 63–78. OPA, 2014. doi:10.4204/EPTCS.160.7.

22 Daniel Gebler and Simone Tini. SOS Specifications of Probabilistic Systems by Uniformly Continuous Operators. In *26th Conference on Concurrency Theory*, volume 42 of *LIPIcs*, pages 155–168. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

23 Hans Hansson and Bengt Jonsson. A Logic for Reasoning about Time and Reliability. *Formal Aspects of Computing*, 6(5):512–535, 1994. doi:10.1007/BF01211866.

24 Bengt Jonsson, Kim G. Larsen, and Wang Yi. Probabilistic Extensions of Process Algebras. In *Handbook of Process Algebra*, pages 685–710. Elsevier, 2001.

25 Leonid V. Kantorovich. On the transfer of masses. *Doklady Akademii Nauk*, 37(2):227–229, 1942. Original article in Russian, translation in Management Science, $5 : 1 - 4(1959)$.

26 Robert M. Keller. Formal Verification of Parallel Programs. *Communications of the ACM*, 19(7):371–384, 1976. doi:10.1145/360248.360251.

27 Ruggero Lanotte, Andrea Maggiolo-Schettini, and Angelo Troina. Time and Probability-based Information Flow Analysis. *IEEE Transactions on Software Engineering*, 36(5):719–734, 2010. doi:10.1109/TSE.2010.4.

28 Ruggero Lanotte, Andrea Maggiolo-Schettini, and Angelo Troina. Weak bisimulation for Probabilistic Timed Automata. *Theoretical Computer Science*, 411(50):4291–4322, 2010. doi:10.1016/j.tcs.2010.09.003.

29 Ruggero Lanotte and Massimo Merro. Semantic Analysis of Gossip Protocols for Wireless Sensor Networks. In *22nd International Conference on Concurrency Theory*, volume 6901 of *LNCS*, pages 156–170. Springer, 2011. doi:10.1007/978-3-642-23217-6_11.

30 Ruggero Lanotte, Massimo Merro, and Simone Tini. Weak Simulation Quasimetric in a Gossip Scenario. In *37th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems*, volume 10321 of *LNCS*, pages 139–155. Springer, 2017. doi:10.1007/978-3-319-60225-7_10.

31 Matteo Mio. Upper-Expectation Bisimilarity and Łukasiewicz μ-Calculus. In *17th International Conference on Foundations of Software Science and Computation Structures*, volume 8412 of *LNCS*, pages 335–350. Springer, 2014. doi:10.1007/978-3-642-54830-7_22.

32 Sandro Rafaeli and David Hutchison. A Survey of Key Management for Secure Group Communication. *ACM Comput. Surv.*, 35(3):309–329, 2003. doi:10.1145/937503.937506.

33 Roberto Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD thesis, MIT, 1995.

34 William J. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton University Press, 1994.

35 Frank van Breugel and J. Worrell. A Behavioural Pseudometric for Probabilistic Transition Systems. *Theor. Comput. Sci.*, 331(1):115–142, 2005. doi:10.1016/j.tcs.2006.05.021.

36 Rob J. van Glabbeek and Peter W. Weijland. Branching Time and Abstraction in Bisimulation Semantics. *Journal of the ACM*, 43(3):555–600, 1996. doi:10.1145/233551.233556.

37 Cédric Villani. *Optimal Transport: Old and New.* Springer, 2009. doi:10.1007/978-3-540-71050-9.