Semantics, bisimulation and congruence results for a general stochastic process operator

Jan Friso Groote[1] Jan Lanik[2]

(1) Departement of Mathematics and Computer Science, Eindhoven University of Technology
Den Dolech 2, Eindhoven, The Netherlands
(2) Faculty of Informatics, Masaryk University, Botanická 68a, Ponava, Brno, Czech Republic
Email: J.F.Groote@tue.nl, xlanik1@fi.muni.cz

Abstract

We introduce a general stochastic process operator $\frac{f}{d:D}p(d)$ which behaves as the process $p(d)$ where the value d is chosen from a data domain D with a probability density determined by f. We require that f is a measurable function from D to $\mathbb{R}^{\geq 0}$ such that $\int_{d\in D} f(d)d\mu_D = 1$. For finite or countable D the function f represents the probability distribution directly. For bigger domains f represents the density function.

We provide a natural operational semantics for a basic process algebra with this operator and define strong stochastic timed bisimulation and general stochastic bisimulation, which due to the potential uncountable nature of D had to be generalised compared to existing notions. We introduce the notion bisimulation resilience, which restricts the use of the language, such that the bisimulation closure of measurable sets is again measurable, and argue that without such a notion stochastic process expressions make little sense. We prove that the bisimulation equivalences are congruences provided the language is bisimulation resilient.

1 Introduction

Our primary motivation comes from our work on a process algebra with data and time (mCRL2, [9]). Our process algebra is on the one hand very straightforward, in the sense that it only contains the minimal set of process operators to model behaviour. But on the other hand it is very rich, in the sense that the operators and allowed data types are as universal and mathematical as possible. Typically, the natural numbers have no largest value, sets are the mathematical notion of sets (e.g., the set of all even numbers can easily be denoted) and all data types can be lifted to functions. The data types are freely usable in processes. For instance, it is possible to write in the language:

$$\sum_{f:\mathbb{R}\to\mathbb{R}} \mathit{receive}(f)\cdot \mathit{forward}(\lambda n{:}\mathbb{Z}.\exists m{:}\mathbb{R}.f(m)>n)\cdot \ldots$$

to *receive* a function f from reals to reals and to *forward* a function from integers to booleans constructed out of f. As the language is very expressive it is easy to write down undecidable conditions. But, if used with care the language turns out to be elegant in modelling even industrially sized systems and the tools are very effective in helping to get insight in these models (see www.mcrl2.org).

As it stands, the language does not allow to express and study stochastic behaviour, although certainly half of the questions that we are asked are about performance, unlikelihood of undesired behaviour and even average behaviour. A typical question from a medical system supplier, which we studied, was which percentage of X-ray pictures will not be processed within 100ms. Another question was about the throughput of an elevator system where the elevators were above each other. The behaviour of such systems are much more conveniently described in process algebras – or most other formalisms stemming from concurrency theory – than in classical queueing theory. However, mathematically, queuing theory is far more developed. From the process perspective, mathematical analysis concentrates around on the one hand, simulation, where any distribution is usable, and on the other hand via Markov chains, which are practically restricted to discrete and exponential distributions.

We desire a theory which allows to describe, study and manipulate with stochastic behaviour on a process level. Therefore, we introduce a simple but very expressive operator. We did not want to allow restrictions on the operator unless self-evident from the problem domain or being a mathematical necessity. We came up with:

$$\frac{f}{d{:}D}p(d)$$

where d is a data variable, D some data domain, p a process in which d can occur and f a probability distribution (not a cumulative distribution). The intuition of the operator is that a value for d is chosen with a probability determined by f after which p happens with this value substituted for d. The same general operator is introduced in [12] with a different notation, which is no coincidence because both this paper and [12] originated from the same discussion on how to add a general stochastic operator to current process algebras. In order to avoid semantical complexities, the operator in [12] is restricted to countable domains and can only be used in a syntactically restricted setting. A tool is available to generate and analyse stochastic state spaces.

The purpose of this paper is a different one, namely to develop and understand a maximally expressive stochastic process algebra. One of the core issues is when such an algebra has a well defined semantics. From measure theory, we know that integration over density functions is only defined when such functions are measurable. We consider processes modulo various bisimulation equivalences. We found out that these are naturally defined if the processes are ‘bisimulation resilient’. This means that if a measurable set of data elements belonging to some set of processes is extended with the data of all bisimilar processes, then this set must be measurable again.

We provide a semantics for our language in terms of stochastic timed automata. Here, states correspond to processes that are stochastically determined, which means that the outgoing transitions from states can be done with certainty. The transitions end in a probability function, which given a set of states tells what the probability is to end up in these states. As already shown in [7, 8] it is necessary to let the probability function work on sets of states, as distributions can be dense. As transitions end in probability functions, the operational rules have to be adapted to reflect this change. As processes can have initial stochastic operators, automata have no initial state, but an initial probability distribution.

Subsequently, we define strong stochastic timed bisimulation for stochastically determined processes, and general stochastic bisimulation for general stochastic processes. With stochastic timed bisimulation we run into the difficulty that the common notion of strong bisimulation for probabilistic processes due to [14] is not adequate. We have to make a small, but crucial extension saying that resulting probability functions must not be compared on bisimulation equivalence classes of states, but on (sometimes uncountable) *unions* of those equivalence classes. Although this may look like a small extension of the definition, it makes a huge difference in the proofs that, becoming notationally more complex, are conceptually much easier than our initial proof attempts. In order to understand intuitively that this extension is needed, we provide an example in terms of processes.

For general processes, we also define a notion of general stochastic bisimulation, but as it is defined on probability functions it hardly looks like a bisimulation. We actually provide this bisimulation in two variants, but we have a strong preference for the second (although our congruence results apply to both of them). The first variant very much resembles open p-bisimulation in [7].

We prove that both notions of bisimulation that we provide are congruences with respect to all process operators that we use. These proofs turn out to be particularly involved and rely heavily on the theory of measurable spaces. A nice place where bisimulations and measure theory meet is lemma 7.13 where it is shown that an arbitrary finite sequence of measurable square sets can be replaced by a disjoint finite sequence of measurable and bisimulation closed square sets covering the same area.

Most articles on stochastic process algebras restrict themselves to finite or exponential distributions. General distributions are found in the work of Josée Desharnais, c.s. [6] but here no operators and congruence results are studied. Absolutely noteworthy is the early work of Pedro D’Argenio c.s. [7, 8] where a process algebra with general distributions over reals setting clocks is given. The clock setting and testing operators of [7] and also the general language is more restricted than ours and in the semantics it is not obvious that sets are always measurable when required. But from all the related work we could find, it is certainly the closest. The work in [7] is also interesting because it provides sets of axioms characterizing structural and open p-bisimulation on processes.

Structure of the paper. In section 2 we give a compact introduction of our timed process algebra with data. In section 3 we give a concise overview of all those elements of basic measurability theory that we require. In section 4 we define stochastic and determined process expressions. Section 5 provides the semantics for these in terms of a timed stochastic automaton. In section 6 the definitions of strong stochastic timed bisimulation, general stochastic bisimulation and bisimulation resilience are given and some elementary properties are proven. Section 7 is the largest and it is used to state and prove that the given bisimulations are congruences. The last section provides some outlooks to further work.

Acknowledgements. We thank Mark Timmer, Suzana Andova, Tim Willemse, Muhammad Atif, and Johann Schuster for fruitful discussions and comments helping us to shape the theory in this paper. Thanks especially go to Marielle Stoelinga who pinpointed a serious error in a late version of the paper.

2 A short description of process algebra with data

We work in the setting of mCRL2, which is a process algebra with data [9, 10]. Processes are constructed from actions which we typically denote by a, b, c, which represent an atomic activity or communication. Actions can carry data parameters, e.g., $a(3)$, $b(\pi, [\mathit{true}, \mathit{false}])$ are the action a carrying the number 3, and the action b carrying the real π and a list with the booleans true and false.

Processes are constructed out of actions using various operators. The most important are the '$\cdot$' and $+$, resp., the sequential and alternative composition operators. A process $p{\cdot}q$ represents a process p and upon termination proceeds with process q. A process $p{+}q$ stands for the process where p or q can be done. The first action determines whether p or q is chosen. So, as an example, the process $a{\cdot}b{+}c{\cdot}d$ can either do an a followed by a b, of a c followed by a d.

There is a time operator $p^{\backprime}t$ with t a non-negative real number, which says that the first action of process p must take place at time t. So, $a^{\backprime}1{\cdot}b^{\backprime}2$ is the process where a happens at exactly time 1 and b at exactly time 2. In the setting of this paper actions cannot happen at the same time, and consecutive actions must happen at consecutive moments in time. In mCRL2, multi-actions are allowed, which are collections of actions that happen at the same instant in time. But as multi-actions are irrelevant for the issues studied in this paper, we do not introduce them here.

A special process is δ, called deadlock or inaction, which is a process that cannot do any action, and which cannot terminate. So, $\delta{\cdot}a = \delta$, because the a cannot be performed. In order to let data influence the actions that can be performed, we use the if-then-else function, compactly denoted by $b{\rightarrow}p{\diamond}q$. Here b is a boolean expression. We use $b{\rightarrow}p$ as the if-then operator.

The process $\delta^{\backprime}t$ is the process that can idle until time t and cannot proceed beyond that point. This is called a time deadlock. Obviously, a process with a time deadlock can never exist in the real world. Related to timed processes is the initialisation operator $t{\gg}p$ which is the process which must start after time t. This operator is required for the operational semantics of the sequential composition operator in a timed setting.

In order to model parallel behaviour there is a parallel operator $p\|q$. This expresses that the actions of p and q can happen in any interleaved fashion. Using a commutative and associative communication function γ it is indicated how actions can communicate. E.g., $\gamma(r, s) = c$ indicates that actions with action labels r and s can happen simultaneously, provided r and s have exactly the same data arguments. The resulting action is called c and also carries the same data as r and s. In order to enforce actions to communicate, there is a block operator $\partial_H(p)$ which blocks all actions with action labels in H. So, a typical pattern is $\partial_{\{r,s\}}(p \parallel q)$ with $\gamma(r, s) = c$, which expresses that actions with labels r and s must communicate into c.

In this paper we adopt an abstract approach towards data, namely, that a data type is a non empty set D on which a number of functions are defined. There are no constraints on the cardinality of D. Typical instances of D that are used frequently are the booleans ($\mathbb{B}$) that contain exactly two elements true and false, various sorts of numbers ($\mathbb{N}^+$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$). But also lists, sets, functions and recursive types are very commonly used. For example sets of lists of reals, or a function from booleans to a recursively defined tree structure are typical data types in a behavioural specification.

There are a number of process operators in mCRL2 that we do not consider in this paper as they do not contribute to this study. One operator that occurs in some examples is the generalised sum operator $\sum_{d:D} p(d)$. It expresses the choice among the processes $p(d)$ for any $d \in D$. This is an interesting but complex operator as it allows to make choice out of an unbounded number of processes. Its interaction with the semantics of the stochastic operator is so tricky, that we decided to leave this operator out of this study.

Another interesting language property that we do not address here is recursive behaviour, which in the setting of mCRL2 is generally described using equations. E.g., the process X defined by $X = a \cdot X$ is the process that can do an action a indefinitely.

3 Mathematical properties of the data domains

In abstract expositions on process algebras with data in the style of mCRL2, data is given by a data algebra $\mathcal{A} = (\mathbf{D}, F)$ where $\mathbf{D}$ is a set of non empty data domains and F contains constants and functions operating on these domains. We typically denote data domains (also called sorts or types) by letters D and E. We assume the existence of the sort $\mathbb{B}$ which contains exactly two elements representing $true$ and $false$ and has an equality predicate $\approx$, where a predicate is just a function that maps into $\mathbb{B}$. Moreover, we assume the existence of the sort $\mathbb{R}$ with reals with at least the predicates $<$,$\leq$,$\approx$ (equality), $\geq$ and $>$ and the constant 0. Reals are used in the time and bounded initialisation operators and booleans are used in the if-then-else operator in processes expressions.

In the this section we identify the required properties that data sorts must have in a stochastic process algebra. We strongly base ourselves on standard measurability theory [17]. In this reference, all important definitions and proofs concerning measures and integration can be found.

We require that all the data domains D are metric extended measurable spaces in the sense that D has a metric ρ_D and a sigma algebra $\Im_D$ with a measure $\mu_D : \Im_D \to \mathbb{R}^{\geq 0} \cup \{\infty\}$. All these notions are defined below. In cases where the domain is obvious from the context we tend to drop the subscripts of ρ_D, $\Im_D$ and μ_D and write the metric, sigma algebra and measure associated to a domain D as ρ, $\Im$ and μ. We introduce the notion of a singleton closed measurable space as a measurable space where individual data elements have a measure.

Given a measurable space we define integrals over measurable functions. This is required to calculate the probability of being in some set of states. For given data domains D and D', we use the product domain $D \times D'$. We indicate how metrics, measures and integrals are lifted to product data types.

First we introduce metrics and the notion of an ϵ-neighbourhood, which we require to indicate that certain events are probable when we are working with dense probability distributions.

Definition 3.1. A *metric* on a data domain D is a function

$$\rho_D : D \times D \to \mathbb{R}^{\geq 0}$$

such that for all $x, y, z \in D$

- $\rho_D(x, y) = 0$ if and only if $x = y$,
- $\rho_D(x, y) = \rho_D(y, x)$, and
- $\rho_D(x, z) \leq \rho_D(x, y) + \rho_D(y, z)$.

Definition 3.2. Let D, D' be data domains with associated metrics $\rho_D, \rho_{D'}$ respectively. The *product metric* $\rho_{D \times D'}$ on the data set $D \times D'$ is defined as

$$\rho_{D \times D'}((a, b), (a', b')) = \sqrt{(\rho_D(a, a'))^2 + (\rho_{D'}(b, b'))^2}$$

for all $a, a' \in D$ and all $b, b' \in D'$.

Definition 3.3. Let D be a data domain with associated metric ρ_D and $\epsilon \in \mathbb{R}$ such that $\epsilon > 0$. For every $d \in D$ we define the *ϵ-neighbourhood* of d as

$$\mathcal{U}_\epsilon(d) = \{x \in D \mid \rho_D(d,x) < \epsilon\}.$$

Next, we introduce the notion of a measurable space, i.e., those subsets of D closed under countable unions and complements. A measure μ_D assigns some size to these subsets. For complex domains the structure of such measurable spaces is not self evident, as exemplified by the Banach-Tarski paradox [2].

Definition 3.4. Let D be a data domain and $\Im_D$ a nonempty family of subsets of D, closed under countable unions and under complements (and hence also under countable intersections). We call $\Im_D$ a *sigma algebra* over D and the pair $(D, \Im_D)$ a *measurable space*. An element $X \in \Im_D$ is called a *measurable set*.

Note that, if $X \in \Im_D$, then $D - X \in \Im_D$, so $D \in \Im_D$, and hence $\emptyset \in \Im_D$.

Definition 3.5. Let D be a data domain. We say, that a sigma algebra $\Im_D$ over D is *generated by* $X \subseteq 2^D$ iff $\Im_D$ is the smallest sigma algebra over D, which contains all the sets in X.

Definition 3.6. Let $(D, \Im_D)$ be a measurable space. A *measure* on $(D, \Im_D)$ is a function $\mu_D : \Im_D \to \mathbb{R}^{\geq 0} \cup \{\infty\}$ satisfying the following two conditions:

1. $\mu_D(\emptyset) = 0$.
2. For any countable sequence of disjoint sets $X_1, X_2, \ldots \in \Im_D$ it holds that

$$\mu_D\left(\bigcup_j X_j\right) = \sum_j \mu_D(X_j).$$

A measure is called *σ-finite* if every $X \subseteq D$ is equal to some countable union $\bigcup_i Y_i$ where $Y_i \subseteq D$ and $\mu_D(Y_i) \neq \infty$. We assume all our measures to be σ-finite.

Throughout this paper we require that we can speak about individual data elements, and therefore we require all our measurable spaces to be singleton closed, as defined below.

Definition 3.7. Let $(D, \Im_D)$ be a measurable space with a metric ρ_D. We say that the $(D, \Im_D)$ is *singleton closed* iff $\Im_D$ contains at least $\{d\}$ and the ϵ-neighbourhood of d for all $d \in D$ and $\epsilon > 0$.

Typically, for continuous domains (e.g., time) the associated measure is the Lebesque measure defined on the Lebesque-measurable subsets and for discrete domains it is a measure $\mu : 2^D \to \mathbb{R}^{\geq 0} \cup \{\infty\}$ such that $\mu(\{d\}) = 1$ for all $d \in D$. It is noteworthy that both measurable spaces are singleton closed.

Definition 3.8. Let $(D, \Im_D)$ and $(D', \Im_{D'})$ be two measurable spaces with measures μ_D and $\mu_{D'}$. Let $\Im_{D \times D'}$ be the sigma algebra over $D \times D'$ generated by the subsets of the form $A \times B$, where $A \in \Im_D$ and $B \in \Im_{D'}$. We define the *product measure* $\mu_{D \times D'} : \Im_{D \times D'} \to \mathbb{R}^{\geq 0} \cup \{\infty\}$ as

$$\mu_{D \times D'}(X) = Sup\left\{\sum_{i=1}^{N} (\mu_D(A_i) \times \mu_{D'}(B_i))\right\},$$

where the supremum is taken over all finite sequences $\{A_i, B_i\}_{i=1}^N$ such that $A_i \in \Im_D$, $B_i \in \Im_{D'}$, $A_i \times B_i \subseteq X$ and the sets $A_i \times B_i$ are mutually disjoint.

Definition 3.9. A *measurable data algebra* $\mathcal{A} = (\mathbf{D}, F)$ is a two tuple where

- $\mathbf{D}$ is a set with elements of the shape $(D, \Im_D, \rho_D)$ where $(D, \Im_D)$ is a singleton closed measurable space and ρ_D is a metric on D,
- F is a set of functions over the data domains in $\mathbf{D}$, and

- The data domains are closed under products. I.e., if there are data domains D and E in $\mathbf{D}$, then there is also a data domain $D \times E$.

In this paper we ignore the difference between syntax and semantics of data types. Separating them can be done in a standard way but would distract from the essence of this paper. Among others, this has as a consequence that we treat the functions in F as syntactical objects to construct data expressions.

Next, we define measurable functions and integrals over these.

Definition 3.10. Let $(D, \Im_D)$ be a measurable space. A function $f : D \to \mathbb{R}^{\geq 0}$ is called a *measurable function* iff $\{d \mid f(d) \in J\} \in \Im_D$ for every open interval $J \subset \mathbb{R}$.

Definition 3.11. Let $S \subseteq D$, where D is some data domain. We define the *characteristic function* of S, $\chi_S : D \to \mathbb{R}^{\geq 0}$, as follows

$$\chi_S(x) = \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{if } x \in D - S. \end{cases}$$

Furthermore, let $\varphi(x)$ be some finite linear combination

$$\varphi(x) = \sum_{j=1}^{N} a_j \chi_{S_j}(x), \quad \text{where } a_1, \ldots, a_N \in \mathbb{R}^{\geq 0}, S_1, \ldots, S_N \in \Im_D. \tag{3.1}$$

Then φ is called *a simple function*.

It is easy to prove that a simple function is measurable. Furthermore, note that a simple function is non-negative.

Definition 3.12. Let $(D, \Im_D)$ be a measurable space with measure μ_D. Let $\varphi : D \to \mathbb{R}^{\geq 0}$ be a simple function as in (3.1) with $A \in \Im_D$. We define the integral

$$\int_A \varphi \, d\mu_D = \sum_{j=1}^{N} a_j \mu_D(S_j \cap A).$$

Let $f : D \to \mathbb{R}^{\geq 0}$ be any measurable function and $A \in \Im_D$. We define the integral

$$\int_A f \, d\mu_D = \sup\{\int_A \varphi \, d\mu_D \mid \ 0 \leq \varphi \leq f, \varphi \text{ is a simple function}\}.$$

Theorem 3.13. Let $(D, \Im_D)$ be a measurable space with measure μ_D. Let $A, B \in \Im_D$, $A \cap B = \emptyset$ and $f : D \to \mathbb{R}^{\geq 0}$ be any measurable function. Then the integral of f is additive in the sense that

$$\int_{A \cup B} f \, d\mu_D = \int_A f \, d\mu_D + \int_B f \, d\mu_D.$$

Theorem 3.14. Let $(D, \Im_D)$ and $(D', \Im'_D)$ be measurable spaces with measure μ_D and μ'_D. Let $A \in \Im_D, B \in \Im'_D$ and let $f : D \to \mathbb{R}^{\geq 0}$ and $g : D' \to \mathbb{R}^{\geq 0}$ are measurable functions. Then

$$\int_{(a,b) \in A \times B} f(a) \cdot g(b) \, d\mu_{D \times D'} = \int_A f \, d\mu_D \cdot \int_B g \, d\mu_{D'}$$

Theorem 3.15. Let $(D, \Im_D)$ be a measurable space with measure μ_D, $f : D \to \mathbb{R}^{\geq 0}$ a measurable function, $X \in \Im_D$ and $X_1 \subseteq X_2 \subseteq \ldots$ a sequence of measurable subsets of X such that $\mu_D(\bigcup_{i=1}^{\infty} X_i) = \mu_D(X)$, then

$$\int_X f d\mu_D = \lim_{i \to \infty} \int_{X_i} f d\mu_D.$$

The following identity relates integrals over a product set $X \in \Im_{A\times B}$ to its constituting domains.

Corollary 3.16. Let $(D, \Im_D)$ and $(D', \Im'_D)$ be measurable spaces with measure μ_D and μ'_D and let $X \subseteq D \times D'$.

$$\int_{(a,b)\in X} f(a,b)\, d\mu_{D\times D'} = Sup\left\{\sum_{i=1}^{N}\left(\int_{a\in A_i}\int_{b\in B_i} f(a,b) d\mu_{D'} d\mu_D\right)\right\}$$

where f is a measurable function defined on the domain $D\times D'$ and the supremum is taken over all possible sequences $\{A_i, B_i\}_1^N$ such that A_i, B_i are measurable and $\bigcup_{i=1}^N A_i \times B_i \subseteq X$ and $A_i \times B_i$ are mutually disjoint.

When $f(a,b) = g(a)\cdot h(b)$ theorem 3.14 simplifies to the following corollary.

Corollary 3.17. Let $(D, \Im_D)$ and $(D', \Im'_D)$ be measurable spaces with measure μ_D and μ'_D and let $X \subseteq D \times D'$.

$$\int_{(a,b)\in X} f(a)\cdot g(b)\, d\mu_{D\times D'} = Sup\left\{\sum_{i=1}^{N}\left(\int_{a\in A_i} f(a) d\mu_D \cdot \int_{b\in B_i} g(b) d\mu_{D'}\right)\right\}$$

where f and g are measurable functions defined on the respective domains D and D', and the supremum is taken over all possible sequences $\{A_i, B_i\}_1^N$ such that A_i, B_i are measurable and $\bigcup_{i=1}^N A_i \times B_i \subseteq X$ and $A_i \times B_i$ are mutually disjoint.

4 A simple stochastic operator

We take the basic process algebraic operators from mCRL2 and enhance them with a simple notation to draw an element from a certain data type with a certain probability. For this we use the following notation (cf. [12] where the same notation has been used):

$$\frac{f}{d{:}D} p,$$

where $f : D \to \mathbb{R}^{\geq 0}$ is a measurable function such that

$$\int_D f d\mu_D = 1.$$

This notation represents the process $p(d)$ where d is drawn from the domain D with a probability distribution, which is defined by the function f. For a finite or countable D the function f represents the distribution directly. For bigger domains it represents the corresponding probability density function. The probability that an element will be drawn from a measurable subset $X \subseteq D$ is defined as

$$Prob(x{\in}X) = \int_X f d\mu_D.$$

Note that with a countable domain D with a measure defined as $\mu_D(\{d\}) = 1$ for all $d \in D$, the probability that a concrete element d is drawn is

$$Prob(x{=}d) = f(d).$$

Example 4.1. The behaviour of a lightbulb which is installed at time st, breaks down at time $st + t$, and which is subsequently repaired at time $st + t + u$ is described by:

$$install^{\varsigma} st \frac{\mathcal{N}_0^\infty(\mu,\sigma^2)}{t{:}\mathbb{R}} break\_down^{\varsigma}(st{+}t)\cdot\frac{\mathcal{N}_0^\infty(\mu,\sigma^2)}{u{:}\mathbb{R}} repair^{\varsigma}(st{+}t{+}u),$$

where t and u are distributed according to the normal distribution $\mathcal{N}_0^\infty(\mu,\sigma^2)$ truncated to the interval $[0,\infty)$.

We consider the following syntax for processes, of which the non stochastic operators have been explained in section 2. Note that a determined (stochastic) process expression is just a process expression, except that there can not be an initial occurrence of the stochastic operator.

Definition 4.2. Let $\mathcal{A} = (\mathbf{D}, F)$ be some data algebra. An expression satisfying the following syntax is called a *(stochastic) process expression*:

$$P \quad ::= \quad a \mid \delta \mid P{+}P \mid P{\cdot}P \mid b{\rightarrow}P{\diamond}P \mid P{}^{c}u \mid u{\gg}P \mid \frac{f}{d{:}D}P \mid P\|P \mid \partial_H(P).$$

An expression satisfying the following syntax is called a *(stochastically) determined process expression*:

$$Q \quad ::= \quad a \mid \delta \mid Q{+}Q \mid Q{\cdot}P \mid b{\rightarrow}Q{\diamond}Q \mid Q{}^{c}u \mid u{\gg}Q \mid Q\|Q \mid \partial_H(Q).$$

Here b is a boolean data expression and u is a data expression of sort u from the data algebra. If we use a domain D in the stochastic operator $\frac{f}{d:D}$ then f always has to be a measurable function from D to $\mathbb{R}^{\geq 0}$ such that $\int_{d\in D} f(d)d\mu_D = 1$. We write $\mathbb{P}$ for the set of process expressions, and $\mathbb{P}_{det}$ for the set of stochastically determined process expressions.

If we can freely use the data types, then it is possible to write down process expressions that have no reasonable meaning in a stochastic sense. In definition 6.2 we provide a general semantical constraint that implies that processes are stochastically well defined. This constraint may limit the use of data expressions that occur in for instance conditions. As our attention is a semantical one, we do not work out these restrictions here, but assume in the sequel that we use data expressions with the appropriate constraints.

We introduce a function det which makes a process stochastically determined by removing all initial occurrences of the stochastic operator.

Definition 4.3. We define the function $det : \mathbb{P} \rightarrow \mathbb{P}_{det}$ recursively on the syntactic structure of processes. Below $p, q \in \mathbb{P}$, $t \in \mathbb{R}$ and $b \in \mathbb{B}$.

$$\begin{array}{lcl}
det(a) & = & a \\
det(\delta) & = & \delta \\
det(p+q) & = & det(p) + det(q) \\
det(p \cdot q) & = & det(p) \cdot q \\
det(b{\rightarrow}p{\diamond}q) & = & b{\rightarrow}det(p){\diamond}det(q) \\
det(p{}^{c}t) & = & det(p){}^{c}t \\
det(t{\gg}p) & = & t{\gg}det(p) \\
det(\frac{f}{d:D}p) & = & det(p) \\
det(p\|q) & = & det(p) \parallel det(q) \\
det(\partial_H(p)) & = & \partial_H(det(p))
\end{array}$$

By induction on the structure of determined process expressions we can prove the following lemma:

Lemma 4.4. Let $p \in \mathbb{P}_{det}$, then $det(p) = p$.

5 Semantics

In this section we define the semantics of our stochastic process language. The semantics of a stochastic process is a timed stochastic automaton, which is defined first. A stochastic automaton has states, which correspond to stochastically determined processes. Furthermore, there are probability functions that, given a set of states, indicate what the probability is to be in one of these states. Especially, there is not an initial state, but an initial probability function, because due to initial stochastic operators, it can be that the initial states are only known with a certain probability distribution.

As we have time, there are two types of transitions, i.e., ordinary transitions labelled with an action and a time tag, and idle transitions, labelled with time, indicating that time can pass. Each ordinary transition goes from a state to a probability function because we sometimes only know the resulting state with a certain probability. Idle transitions go neither to a state nor to a probability function.

After providing the general definition of a timed stochastic automaton, we define the semantics of a process expression in terms of such an automaton using a set of structured operational semantical rules.

Definition 5.1. A *timed stochastic automaton* is a five tuple $(S, Act, \mathcal{F}, \longrightarrow, \rightsquigarrow, f_0, T)$ where

- S is a set of states.
- Act is a set of actions.
- $\mathcal{F}$ is a set of *probability functions* $f : 2^S \rightarrow [0,1] \cup \{\bot\}$ that can assign a probability to sets of states. If the probability is not defined for some set of states X, then $f(X) = \bot$.
- $\longrightarrow \subseteq S \times Act \times \mathbb{R}^{>0} \times \mathcal{F}$ is a *transition relation*. The expression $s \xrightarrow{a}_t f$ says that a traversal is made from state s to probability function f by executing action a at time t.
- $\rightsquigarrow \subseteq S \times \mathbb{R}^{>0}$ is the *idle relation*. The predicate $s \rightsquigarrow_t$ expresses that it is possible to idle until and including time t in state s.
- f_0 is the *initial probability function*.
- $T \subseteq S$ is the set of *terminating states*.

Every timed transition system must satisfy the *progress* and *density* requirements. Let s, s' and s'' be some states in S, a and a' some actions in Act and $t, t' \in \mathbb{R}^{>0}$ some points in time. The progress requirement says that

$$\text{if } s \xrightarrow{a}_t s' \xrightarrow{a'}_{t'} s'' \text{ or } s \xrightarrow{a}_t s' \rightsquigarrow_{t'}, \text{ then } t' > t.$$

The density requirement expresses that for any action $a \in Act$, states $s, s' \in S$ and time $t \in \mathbb{R}^{>0}$

$$\text{if } s \xrightarrow{a}_t s' \text{ or } s \rightsquigarrow_t, \text{ then } s \rightsquigarrow_{t'}$$

for any $0 < t' \leq t$.

Below we define how a stochastic timed automaton is obtained from a stochastic process expression. The first main ingredient is the function $Stoch$ (see definition 5.6). The probability function $Stoch(p)$ applied to a set of states X gives the probability that in process p one can end up in one of the states in X. Typically, $Stoch(p)$ represents the initial probability function of the timed probabilistic automaton which is the semantics of p.

All definitions up to definition 5.6 are required to define $Stoch$. The function $stochvar(p)$ provides the initial stochastic domains in process p. If there are no stochastic domains, when p is a stochastically determined process, then $stochvar(p) = \{\emptyset\}$, i.e., the set containing the empty set. The density function $[\![p]\!]$ applied to an element of a data domain, provides the probability that this element is chosen in the initial stochastic operator in p. Using a function $\mathcal{D}_p$ states are translated to the matching data elements for p.

Definition 5.2. Let p be an arbitrary process expression. We define the *domain of its unguarded stochastically bounded data variables* $stochvar(p)$ inductively as follows:

$$\begin{array}{lcl}
stochvar(a) & = & \{\emptyset\} \\
stochvar(\delta) & = & \{\emptyset\} \\
stochvar(p + q) & = & stochvar(p) \times stochvar(q) \\
stochvar(p \cdot q) & = & stochvar(p) \\
stochvar(b \rightarrow p \diamond q) & = & stochvar(p) \times stochvar(q) \\
stochvar(p^{\varsigma}t) & = & stochvar(p) \\
stochvar(t \gg p) & = & stochvar(p) \\
stochvar(\frac{f}{d:D} p) & = & D \times stochvar(p) \\
stochvar(p \| q) & = & stochvar(p) \times stochvar(q) \\
stochvar(\partial_H(p)) & = & stochvar(p)
\end{array}$$

By induction on the structure of determined process expressions we can prove the following lemma.

Lemma 5.3. If $p \in \mathbb{P}_{det}$, then $stochvar(p) = \{\emptyset\}$.

Definition 5.4. Let p be a stochastic process expression. The *density function* of p, denoted by $[\![p]\!]$, is a function

$$[\![p]\!] : stochvar(p) \longrightarrow \mathbb{R},$$

which is inductively defined as follows:

$$\begin{array}{lcl}
[\![a]\!] & = & \lambda d{:}\{\emptyset\}.1 \\
[\![\delta]\!] & = & \lambda d{:}\{\emptyset\}.1 \\
[\![p+q]\!] & = & \lambda \vec{d}{:}stochvar(p), \vec{e}{:}stochvar(q).[\![p]\!](\vec{d})\cdot[\![q]\!](\vec{e}) \\
[\![p \cdot q]\!] & = & [\![p]\!] \\
[\![b {\longrightarrow} p {\diamond} q]\!] & = & \lambda \vec{d}{:}stochvar(p), \vec{e}{:}stochvar(q).[\![p]\!](\vec{d})\cdot[\![q]\!](\vec{e}) \\
[\![p^{\scriptscriptstyle\langle}t]\!] & = & [\![p]\!] \\
[\![t{\gg}p]\!] & = & [\![p]\!] \\
[\![\frac{f}{d:D}p]\!] & = & \lambda d{:}D, \vec{d}{:}stochvar(p).f(d)\cdot[\![p(d)]\!](\vec{d}) \\
[\![p \| q]\!] & = & \lambda \vec{d}{:}stochvar(p), \vec{e}{:}stochvar(q).[\![p]\!](\vec{d})\cdot[\![q]\!](\vec{e}) \\
[\![\partial_H(p)]\!] & = & [\![p]\!]
\end{array}$$

Note that for any stochastic process expression p it is the case that $[\![p]\!]$ is a measurable function on $(stochvar(p), \Im_{stochvar(p)})$. This is due to the fact that each f in a stochastic operator is a measurable function, and the product of measurable spaces is again a measurable space (see section 3). Observe also that for any stochastically determined process expression p we have

$$[\![p]\!](\emptyset) = 1.$$

Definition 5.5. Let $X \subseteq S$ be an arbitrary set of determined processes and p an arbitrary (not necessarily determined) process. We define the *data projection of X w.r.t. p* as follows

$$\mathcal{D}_p(X) = \{d \in stochvar(p) \mid det(p)(d) \in X\}.$$

Definition 5.6. Let p be a stochastic process expression. We define $Stoch(p)$ by

$$Stoch(p)(X) = \begin{cases} \displaystyle\int_{\mathcal{D}_p(X)} [\![p]\!]\, d\mu_{stochvar(p)} & \text{if } \mathcal{D}_p(X) \text{ is a measurable set,} \\ \bot & \text{otherwise.} \end{cases}$$

In the tables 1, 2, 3 rules are given for the operational semantics. In these tables we use the following auxiliary notion of a termination detecting distribution function. This function yields probability 1 on a set of states iff there is a terminating state among them.

Definition 5.7. Let $S = \mathbb{P}_{det} \cup \{\checkmark\}$. The *termination checking distribution function* $f_\checkmark$ is defined as follows where $X{\in}2^S$ is a set of states.

$$f_\checkmark(X) = \begin{cases} 1 & \text{if } \checkmark \in X, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, we extend the definitions of $stochvar$ and det to the termination symbol $\checkmark$.

$$\begin{array}{rcl}
stochvar(\checkmark) & = & \{\emptyset\}, \\
det(\checkmark) & = & \checkmark.
\end{array}$$

Definition 5.8. Let $\mathcal{A} = (\mathbf{D}, F)$ be a measurable data algebra and let p be a process expression. The semantics of a process p is defined by the timed stochastic automaton $(S, Act, \mathcal{F}, \longrightarrow, \rightsquigarrow, f_0, T)$ of which the components are given by

$\frac{}{a \xrightarrow{a}_t f_{\checkmark}}\ t{>}0$	$\frac{}{a \rightsquigarrow_t}$	$\frac{}{\delta \rightsquigarrow_t}$
$\frac{p \xrightarrow{a}_t f}{p{+}q \xrightarrow{a}_t f}$	$\frac{p \rightsquigarrow_t}{p{+}q \rightsquigarrow_t}$	
$\frac{q \xrightarrow{a}_t f}{p{+}q \xrightarrow{a}_t f}$	$\frac{q \rightsquigarrow_t}{p{+}q \rightsquigarrow_t}$	
$\frac{p \xrightarrow{a}_t f_{\checkmark}}{p{\cdot}q \xrightarrow{a}_t Stoch(t{\gg}q)}$	$\frac{p \xrightarrow{a}_t f}{p{\cdot}q \xrightarrow{a}_t \lambda U{:}2^S.f(\{r \mid r{\cdot}q{\in}U\})}\ f \neq f_{\checkmark}$	$\frac{p \rightsquigarrow_t}{p{\cdot}q \rightsquigarrow_t}$
$\frac{p \xrightarrow{a}_t f}{(b{\rightarrow}p{\diamond}q) \xrightarrow{a}_t f}\ (b{\approx}true)$	$\frac{p \rightsquigarrow_t}{(b{\rightarrow}p{\diamond}q) \rightsquigarrow_t}\ (b{\approx}true)$	
$\frac{q \xrightarrow{a}_t f}{(b{\rightarrow}p{\diamond}q) \xrightarrow{a}_t f}\ (b{\approx}false)$	$\frac{q \rightsquigarrow_t}{(b{\rightarrow}p{\diamond}q) \rightsquigarrow_t}\ (b{\approx}false)$	

Table 1: Operational rules for the basic operators

$\frac{p \xrightarrow{a}_t f}{p\text{‹}t \xrightarrow{a}_t f}$	$\frac{p \rightsquigarrow_t}{p\text{‹}u \rightsquigarrow_t}\ (t \leq u)$
$\frac{p \xrightarrow{a}_t f}{u{\gg}p \xrightarrow{a}_t f}\ (u \leq t)$	
$\frac{p \rightsquigarrow_t}{u{\gg}p \rightsquigarrow_t}$	$\frac{}{u{\gg}p \rightsquigarrow_t}\ (t \leq u)$

Table 2: Operational rules for the time operator and the bounded initialisation operator

- $S = \mathbb{P}_{det} \cup \{\checkmark\}$.
- $\mathcal{F}$ is the set of all probability functions $f : 2^S \to [0,1] \cup \{\perp\}$.
- $\longrightarrow$ and $\rightsquigarrow$ are recursively defined by the inference rules in tables 1, 2, 3. The multiplication used in the rule for the parallel operator in table 3 between possibly undefined probabilities is undefined if one or both of its constituents is undefined.
- $f_0 = Stoch(p)$.
- $T = \{\checkmark\}$.

$$\frac{p \xrightarrow{a}_t f_{\checkmark},\ q \rightsquigarrow_t}{p\|q \xrightarrow{a}_t \mathit{Stoch}(t{\gg}q)} \qquad \frac{p \xrightarrow{a}_t f,\ q \rightsquigarrow_t}{p\|q \xrightarrow{a}_t \lambda U{:}2^S.f(\{r|(r\|t{\gg}q){\in}U\})}\ f \neq f_{\checkmark}$$

$$\frac{p \rightsquigarrow_t,\ q \xrightarrow{a}_t f_{\checkmark}}{p\|q \xrightarrow{a}_t \mathit{Stoch}(t{\gg}p)} \qquad \frac{p \rightsquigarrow_t,\ q \xrightarrow{a}_t f}{p\|q \xrightarrow{a}_t \lambda U{:}2^S.f(\{r|(t{\gg}p\|r){\in}U\})}\ f \neq f_{\checkmark}$$

$$\frac{p \xrightarrow{b}_t f, \quad q \xrightarrow{c}_t g}{p\|q \xrightarrow{a}_t \lambda U{:}2^S.f(\{r|\exists s.r\|s \in U\}){\cdot}g(\{s|\exists r.r\|s \in U\})}\ \gamma(b,c) = a,\ f \neq f_{\checkmark},\ g \neq f_{\checkmark}$$

$$\frac{p \xrightarrow{b}_t f, \quad q \xrightarrow{c}_t f_{\checkmark}}{p\|q \xrightarrow{a}_t f}\ \gamma(b,c) = a,\ f \neq f_{\checkmark}$$

$$\frac{p \xrightarrow{b}_t f_{\checkmark}, \quad q \xrightarrow{c}_t g}{p\|q \xrightarrow{a}_t g}\ \gamma(b,c) = a,\ g \neq f_{\checkmark}$$

$$\frac{p \xrightarrow{b}_t f_{\checkmark}, \quad q \xrightarrow{c}_t f_{\checkmark}}{p\|q \xrightarrow{a}_t f_{\checkmark}}\ \gamma(b,c) = a$$

$$\frac{p \rightsquigarrow_t,\ q \rightsquigarrow_t}{p\|q \rightsquigarrow_t} \qquad \frac{p \xrightarrow{a}_t f}{\partial_H(p) \xrightarrow{a}_t \lambda U{:}2^S.f(\{r|(\partial_H(r){\in}U\})}\ a \notin H \qquad \frac{p \rightsquigarrow_t}{\partial_H(p) \rightsquigarrow_t}$$

Table 3: Structured operational semantics for the parallel and the encapsulation operator

6 Stochastic timed bisimulation and general stochastic bisimulation

In this section two equivalences to relate stochastic processes are given and some elementary properties about them are proven.

The first equivalence only relates determined stochastic processes that form the states of automata constituting the semantics of stochastic processes. The equivalence is formulated as a bisimulation, and it is inspired by the classical definition from [14]. There is a notable and important difference namely that the resulting probability functions must be equal for all *unions* of equivalence classes. This is required to deal with the potentially continuous nature of our data domains. After the definition we provide a motivating example to illustrate this necessity.

In definition 6.9 we define general stochastic bisimulation for arbitrary processes which is the core equivalence we are interested in. As arbitrary processes are interpreted as probability distributions, general stochastic bisimulation is defined in terms of probability functions and therefore it looks quite different from an ordinary definition of bisimulation.

Definition 6.1. Let $(S, Act, \mathcal{F}, \longrightarrow, \rightsquigarrow, f_0, T)$ be a stochastic automaton as defined in definition 5.8. We say that an equivalence relation R is a *strong stochastic timed bisimulation* iff it satisfies for all states $s, s' \in S$ such that sRs'

if $s \xrightarrow{a}_t f$ for some $f \in \mathcal{F},$ then there is an $f' \in \mathcal{F}$ such that
$s' \xrightarrow{a}_t f'$ and for all $X \subseteq S/R$ it holds that $f(\bigcup X) = f'(\bigcup X)$.

Furthermore,

if $s \rightsquigarrow_t,$ then $s' \rightsquigarrow_t$.

Finally,

if $s \in T,$ then $s' \in T$.

We say that two states $s, s' \in S$ are *strongly stochastically timed bisimilar*, notation $s \underline{\leftrightarrow}_{dt} s'$, iff there is a strong stochastic timed bisimulation R such that sRs'. The relation $\underline{\leftrightarrow}_{dt}$ is called *strong stochastic timed bisimulation equivalence*.

For closed stochastically determined process expressions p and q we say that they are *strongly stochastically timed bisimilar*, notation $p \underline{\leftrightarrow}_{dt} q$, if p and q are strongly stochastically timed bisimilar states. If p and q are open stochastically determined process expressions, then we say that they are *strongly stochastically timed bisimilar*, notation $p \underline{\leftrightarrow}_{dt} q$, iff they are *strongly stochastically timed bisimilar* for all closed instances.

The necessity of using unions of equivalence classes in the definition above can be seen by considering the following two determined stochastic processes:

$$a_1 \cdot \frac{f}{r{:}\mathbb{R}} a_2(r) \qquad \text{and} \qquad a_1 \cdot \frac{f}{r{:}\mathbb{R}} a_2(r+1) \tag{6.1}$$

where f is some continuous distribution such that for every r it is the case that $f(r) = 0$. The two probability functions that are reached after performing an a_1 action in both processes is given by respectively:

$$f_1 = \mathit{Stoch}(\frac{f}{r{:}\mathbb{R}} a_2(r)) \qquad \text{and} \qquad f_2 = \mathit{Stoch}(\frac{f}{r{:}\mathbb{R}} a_2(r+1)).$$

Every bisimulation equivalence class $X \in S/_{\underline{\leftrightarrow}_{rt}}$ contains $a_2(r)$ for some r. Therefore, it is the case that $f_1(X) = 0$ and $f_2(X) = 0$. So, if a single equivalence class were used in definition 6.1 both processes in formula (6.1) would be considered equivalent. Using unions of equivalence classes this problem is very naturally resolved.

Definition 6.1 has an undesired feature, namely that it defines that processes are bisimilar when actions can happen with undefined probabilities. Consider the following two processes.

$$p_1 = a_1 \cdot \frac{f}{d{:}D} b(d) \rightarrow a_2 \diamond \delta,$$

$$p_2 = a_1 \cdot \frac{f}{d{:}D} b(d) \rightarrow \delta \diamond a_2$$

where b is a non measurable predicate on d. For the real numbers b could represent membership in some Vitali set. Both processes are stochastically timed bisimilar, because after doing an a_1 action, the probability of ending up in the bisimulation equivalence class where a single a_2 action can be performed can not be measured. The probability in both cases is undefined, and therefore equal.

One might try to avoid equating the processes p_1 and p_2 by stating that processes cannot be equal whenever their probabilities are undefined. But this has as a consequence that bisimulation is not reflexive. In such a case p_1 is not equal to itself, because the probabilities of doing an a_2 after doing the a_1 action cannot be determined.

In order to avoid such anomalies we introduce the following constraint. The lemma following the theorem explains the use of the definition, saying that for all bisimulation closed sets of states, the associated set of data values is always measurable.

Definition 6.2. Let $\mathcal{A}$ be a measurable data algebra and p be a process expression. We say that p is *bisimulation resilient* with respect to $\mathcal{A}$ iff for all stochastic process expressions p and every measurable sets $A \subseteq \mathit{stochvar}(p)$ the set

$$\{e \in \mathit{stochvar}(p) \mid \exists d \in A.\mathit{det}(p)(e) \underline{\leftrightarrow}_{dt} \mathit{det}(p)(d)\}$$

is also a measurable set.

Lemma 6.3. Let $\mathcal{A}$ be a measurable data algebra and p a process expression that is bisimulation resilient with respect to $\mathcal{A}$. For all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ the set $\mathcal{D}_p(\bigcup X)$ is measurable.

The next lemma is a very useful workhorse to prove relations to be stochastically timed bisimilar as it summarises reasoning occurring in almost every proof.

Lemma 6.4. Let $\mathcal{F}$ be a set of functions from 2^S to $[0,1] \cup \{\bot\}$ and let $R, R' \subseteq S \times S$ be two equivalence relations such that $R \subseteq R'$. If for arbitrary $f, f' \in \mathcal{F}$ such that for all $X{\subseteq}S/R$ it is the case that $f(\bigcup X){=}f'(\bigcup X)$, it also holds that for all $Y{\subseteq}S/R'$ it is the case that $f(\bigcup Y){=}f'(\bigcup Y)$.

Proof. As both R and R' are equivalence relations and R' contains R, every equivalence class in S/R' must be composed of one or more equivalence classes from S/R. Hence, for all $X{\in}S/R'$ there are $H_X \subseteq S/R$ such that $X = \bigcup H_X$. Take an arbitrary $Y \subseteq S/R'$, i.e. $Y = \bigcup_{i \in I} Y_i$, where $Y_i \in S/R'$, and arbitrary $f, f'{\in}\mathcal{F}$ such that for all $H{\subseteq}S/R$ it is the case that $f(\bigcup H){=}f'(\bigcup H)$. Then it holds

$$f(Y) = f\left(\bigcup_{i \in I} Y_i\right) = f\left(\bigcup_{i \in I} \bigcup H_{Y_i}\right) = f'\left(\bigcup_{i \in I} \bigcup H_{Y_i}\right) = f'\left(\bigcup_{i \in I} Y_i\right) = f'(Y)$$

because $\{H_{Y_i} \mid i \in I\} \subseteq S/R$. □

The following self evident theorem is provided explicitly because its proof is not self evident. Moreover, history shows that given the complexity of the definition of strong stochastic timed bisimulation, such theorems are not always correct and therefore worthy of being provided explicitly. The same holds for lemma 6.6 which is also very elementary.

Theorem 6.5. Strong stochastic timed bisimulation equivalence ($\underline{\leftrightarrow}_{dt}$) is an equivalence relation.

Proof. Reflexivity and symmetry follow directly from the fact that a strong stochastic timed bisimulation relation is an equivalence relation. The proof of transitivity goes as follows.

Assume for arbitrary states $s, s', s'' \in S$ that $s \underline{\leftrightarrow}_{dt} s'$ and $s' \underline{\leftrightarrow}_{dt} s''$. This means that there are strong stochastic timed bisimulation relations R and R' such that sRs' and $s'R's''$. Below we show that the transitive closure of $R \cup R'$, which we call $\tilde{R}$, is also a strong stochastic timed bisimulation relation. The relation $\tilde{R}$ clearly relates s and s'', so $s \underline{\leftrightarrow}_{dt} s''$.

So, we are to show that $\tilde{R}$ is a strong stochastic timed bisimulation. Assume that there are some states s and s' (different from those in the previous paragraph) such that $s\tilde{R}s'$. This means that s and s' are related via a sequence

$$sR_1s_1R_2s_2 \ldots s_{n-1}R_ns' \tag{6.2}$$

where R_i is either R or R'. By an inductive argument on (6.2) it follows that when $s \rightsquigarrow_t$, then $s' \rightsquigarrow_t$, and with the same argument that if $s{\in}T$, then $s'{\in}T$.

Using (6.2) it also follows that if $s \xrightarrow{a}_t f$, then $s_1 \xrightarrow{a} f_1$, $s_2 \xrightarrow{a} f_2$, etc., until ultimately $s' \xrightarrow{a}_t f'$. In order to prove that $\tilde{R}$ is a strong stochastic timed bisimulation, we must show for any $X{\subseteq}S/\tilde{R}$ that $f(\bigcup X) = f'(\bigcup X)$. We know that R, R' and $\tilde{R}$ are equivalence relations, $R, R' \subseteq \tilde{R}$ and for arbitrary f_i, f_{i+1} we have $\forall X \subseteq S/R.f_i(\bigcup X) = f_{i+1}(\bigcup X)$ or $\forall X \subseteq S/R'.f_i(\bigcup X) = f_{i+1}(\bigcup X)$. Therefore, from lemma 6.4 it follows $\forall X \subseteq S/\tilde{R}.f_i(\bigcup X) = f_{i+1}(\bigcup X)$.

By inductively applying this argument using (6.2) it follows that $f(\bigcup X) = f'(\bigcup X)$. □

Lemma 6.6. Strong stochastic timed bisimulation equivalence ($\underline{\leftrightarrow}_{dt}$) is a strong stochastic timed bisimulation relation.

Proof. From theorem 6.5 we have that $\underline{\leftrightarrow}_{dt}$ is an equivalence relation. So, choose arbitrary $(p,q){\in}\underline{\leftrightarrow}_{dt}$. From the definition of $\underline{\leftrightarrow}_{dt}$ it follows that there is some strong stochastic timed bisimulation R such that $(p,q) \in R$.

Therefore if $p \xrightarrow{a}_t f$, then there is an f' such that $q \xrightarrow{a}_t f'$ and for all $X \subseteq S/R$ it holds that $f(\bigcup X) = f'(\bigcup X)$. As $R \subseteq \underline{\leftrightarrow}_{dt}$, using lemma 6.4 we get $f(\bigcup Y) = f'(\bigcup Y)$ for all $Y \subseteq S/_{\underline{\leftrightarrow}_{dt}}$. Furthermore from $(p,q) \in R$ it follows that if $p \rightsquigarrow_t,$ then $q \rightsquigarrow_t$ and if $p \in T,$ then $q \in T$. So, we have shown that $\underline{\leftrightarrow}_{dt}$ is a strong stochastic timed bisimulation relation. □

The following lemma says that $f_{\checkmark}$ is in a sense unique, because using the operational semantics, it can only be 'simulated' by $f_{\checkmark}$ and no other probability function.

Lemma 6.7. Consider two stochastically determined process expressions p and q. If $p{\leftrightarrows}_{dt}q$ and $p \xrightarrow{a}_t f_{\checkmark}$, then $q \xrightarrow{a}_t f_{\checkmark}$.

Proof. As $p{\leftrightarrows}_{dt}q$ and $p \xrightarrow{a}_t f_{\checkmark}$, we find for some probability function f that $q \xrightarrow{a}_t f$ such that for all $X{\subseteq}S/_{\leftrightarrows_{dt}}$ it is the case that $f(\bigcup X){=}f_{\checkmark}(\bigcup X)$. Consider the set $\mathbf{S}$ of all bisimulation classes, except $\{\checkmark\}$, defined by $\mathbf{S}{=}\{U{\subseteq}S \mid U{\in}S/_{\leftrightarrows_{dt}}\}$. So, $f(\bigcup\mathbf{S}){=}f_{\checkmark}(\bigcup\mathbf{S}){=}0$ and $f((\bigcup\mathbf{S}){\cup}\{\checkmark\}){=}f_{\checkmark}((\bigcup\mathbf{S}){\cup}\{\checkmark\}){=}1$. With induction on the derivation of $q \xrightarrow{a}_t f$ it can be shown that if there is a $X{\subseteq}S$ such that $\checkmark{\notin}X$ and $f(X){\neq}f(X \cup \{\checkmark\})$, then $f{=}f_{\checkmark}$. □

Before we are ready to provide our main equivalence notion, we need one final preparatory definition to determine whether there is a data element d such that it is conceivable to end up in $p(d)$. If d is a dense domain, $Stoch(p)(\{d\})$ is most likely equal to 0 for any datum d. In order to determine whether $p(d)$ is possible, we look at an arbitrary small epsilon environment $\mathcal{U}_\epsilon(d)$ around d and check that the probability to be in this environment is larger than 0.

Definition 6.8. Let p be an arbitrary stochastic process. We say that $\vec{d}{\in}stochvar(p)$ is *possible* in p iff for all real numbers $\epsilon{>}0$ it holds

$$\int_{\mathcal{U}_\epsilon(\vec{d})} [\![p]\!] \ d\mu > 0,$$

where $\mathcal{U}_\epsilon(\vec{d})$ is the ϵ-neighbourhood of d with respect to $\rho_{stochvar(p)}$ (see definition 3.3).

We are now ready to provide our main equivalence between arbitrary stochastic processes.

Definition 6.9. Let p, q be two closed stochastic process expressions. We say that p and q are *generally stochastically bisimilar* (denoted $p{\leftrightarrows}q$) iff for all $X{\subseteq}S/_{\leftrightarrows_{dt}}$ it holds that

$$Stoch(p)(\bigcup X) = Stoch(q)(\bigcup X).$$

and for all *possible* d in p there exists some *possible* e in q such that

$$det(p)(d) \leftrightarrows_{dt} det(q)(e)$$

The relation $\leftrightarrows$ is called *general stochastic bisimulation*.

Note that it is immediately obvious from the definition that general stochastic bisimulation is an equivalence relation.

Corollary 6.10. If $p \leftrightarrows q$ then for all $X \subseteq S/_{\leftrightarrows_{dt}}$ it holds that

$$\mathcal{D}_p(\bigcup X) \text{ is measurable iff } \mathcal{D}_q(\bigcup X) \text{ is measurable.}$$

Proof. This corollary is a direct consequence of definition 5.6. □

It is possible to work with a weaker definition of general stochastic bisimulation, which consists of only the first condition of definition 6.9. Our inspection indicates that all congruence results carry over to this setting.

However, for the weaker definition the generalised sum operator is not a congruence. This can be seen by the following example. The notation $r{\approx}x$ represents equality between the data elements r and x.

$$p_x = \frac{f}{r{:}\mathbb{R}}(r{\approx}x) \to a \diamond \delta \qquad \text{and} \qquad q = \frac{f}{r{:}\mathbb{R}}\delta$$

where f is some continuous distribution and μ is the Lebesque measure with $f(r) = 0$ and $\int_{\mathcal{U}_\epsilon(r)} f d\mu > 0$ (i.e., r is possible in p_x) for any $r \in \mathbb{R}$. Note that most common continuous distributions satisfy this.

The processes p_x and q are not generally stochastically bisimilar, as the 'possible' a action of p_x cannot be mimicked by q. But they are related in the weaker variant because the class of stochastically determined processes bisimilar to $x{\approx}x{\to}a{\diamond}\delta$ has probability zero.

However, if we put the generalised sum operator in front of both sides, we obtain

$$\sum_{x:\mathbb{R}} \frac{f}{r:\mathbb{R}}(r{\approx}x) \to a \diamond \delta \qquad \text{and} \qquad \sum_{x:\mathbb{R}} \frac{f}{r:\mathbb{R}}\delta. \tag{6.3}$$

The process at the left can do an a step with a positive probability, although without a precise semantics the argument is still intuitive. Take for instance $f(r) = e^{-r}$ for $r > 0$, otherwise $f(r) = 0$. Then the probability of being able to do an a action in the process at the left of equation (6.3) is 1 minus the probability that no a step can be done:

$$1 - \prod_{r:\mathbb{R}}(1 - f(r)d\mu_r) = 1 - e^{\int_0^\infty f(r)d\mu_r} = 1 - e^{-1} \approx 0.632.$$

The process at the right of equation (6.3) can do no a step at all. So, the so desired congruence property does not hold, which is of course due to the fact that the sum operator can combine an unbounded number of processes.

The generalised sum operator is a very important operator. Therefore we decided to consider processes p_x and q non bisimilar, which is ensured by the second condition in the definition of general stochastic bisimulation.

The following lemma tells us that for determined stochastic processes our definitions of bisimulation coincide.

Lemma 6.11. Two bisimulation resilient, stochastically determined processes p and q are generally stochastically bisimilar if and only if they are strongly stochastically bisimilar, i.e.,

$p \leftrightarrows q$ if and only if $p \leftrightarrows_{dt} q$.

Proof. Let p, q be bisimulation resilient and stochastically determined processes. Therefore for arbitrary $X{\subseteq}S/_{\leftrightarrows_{dt}}$ it holds

$$\mathit{Stoch}(p)(X) = \begin{cases} 1 & \text{iff } p \in X \\ 0 & \text{iff } p \notin X \end{cases} \qquad \mathit{Stoch}(q)(X) = \begin{cases} 1 & \text{iff } q \in X \\ 0 & \text{iff } q \notin X \end{cases}$$

1. Let $p{\leftrightarrows}q$. Then for all $Y{\subseteq}S/_{\leftrightarrows_{dt}}$ it holds $\mathit{Stoch}(p)(\bigcup Y){=}\mathit{Stoch}(q)(\bigcup Y)$. In particular, for all $C{\in}S/_{\leftrightarrows_{dt}}$ we have $\mathit{Stoch}(p)(C){=}\mathit{Stoch}(q)(C)$. Therefore either $\mathit{Stoch}(p)(C){=}\mathit{Stoch}(q)(C){=}1$ and both p, q are in C or $\mathit{Stoch}(p)(C){=}\mathit{Stoch}(q)(C){=}0$ and both p, q are not in C. Therefore $p{\leftrightarrows}_{dt}q$.
2. Let $p{\leftrightarrows}_{dt}q$. Then obviously the second case of definition 6.9 is satisfied as $det(p){=}p$ and $det(q){=}q$. For the first case, observe that for all $Y{\subseteq}S/_{\leftrightarrows_{dt}}$ either both p and q are in $\bigcup Y$ or neither of them is. Hence, either $\mathit{Stoch}(p)(\bigcup Y) = 1 = \mathit{Stoch}(q)(\bigcup Y)$ or $\mathit{Stoch}(p)(\bigcup Y) = 0 = \mathit{Stoch}(q)(\bigcup Y)$. Therefore, $p{\leftrightarrows}q$.

By putting both direction together this lemma is proven. □

7 The stochastic bisimulation relations are congruences

The following section is completely devoted to proving that strong stochastic timed bisimulation and general stochastic bisimulation are congruences. There is one snag, namely that the sequential composition operator for determined processes allows a general stochastic process expression as its second argument. Therefore, the congruence theorem for the sequential composition for strong stochastic timed bisimulation (theorem 7.11) has the slightly unusual formulation:

$$p{\leftrightarrows}_{dt}p' \text{ and } p{\leftrightarrows}q' \text{ implies } p{\cdot}q{\leftrightarrows}_{dt}p'{\cdot}q'.$$

All other formulations are exactly as expected.

The proofs are quite technical. For strong stochastic timed bisimulation, a relation R is given that is proven to satisfy all properties of a bisimulation. A complication is that R must be an equivalence relation. This is achieved by considering the transitive closure of R. Definition 7.1 and lemma 7.2 are tools to compactly deal with the typical reasoning that occurs in every congruence proof of strong timed bisimulation.

The congruence results for general stochastic bisimulation have as most complex aspect that they use multiplication of probability functions. These can be calculated using corollary 3.17 as the supremum of a finite approximation of squares $\{D_i, E_i\}_{i=1}^{N}$. However, in the proofs it is essential that the domains D_i and E_i are bisimulation closed (cf. definition 7.12) and pairwise disjoint. Lemma 7.13 shows that a longer but still finite sequence $\{D_j^*, E_j^*\}_{j=1}^{M}$ with the required properties can be constructed.

Definition 7.1. Let $(S, Act, \mathcal{F}, \longrightarrow, \rightsquigarrow, f_0, T)$ be a stochastic automaton. We say that a symmetric and transitive relation $\rho \subseteq S \times S$ is a *partial strong stochastic timed bisimulation* iff for all states $s, s' \in S$ such that $s \rho s'$ it satisfies

$$\text{if } s \xrightarrow{a}_t f \text{ for some } f \in \mathcal{F}, \text{ then there is an } f' \in \mathcal{F} \text{ such that}$$
$$s' \xrightarrow{a}_t f' \text{ and for all } X \subseteq S/_{(\rho \cup \leftrightarrows_{dt})^*} \text{ it holds that } f(\bigcup X) = f'(\bigcup X).$$

Furthermore,

$$\text{if } s \rightsquigarrow_t, \text{ then } s' \rightsquigarrow_t .$$

Finally,

$$\text{if } s \in T, \text{ then } s' \in T.$$

The expression $(\rho \cup \leftrightarrows_{dt})^*$ denotes the transitive closure of $\rho \cup \leftrightarrows_{dt}$. Note that $(\rho \cup \leftrightarrows_{dt})^*$ is an equivalence relation. This follows from the the symmetry of both ρ and $\leftrightarrows_{dt}$, from the reflexivity of $\leftrightarrows_{dt}$ and from the fact that it is a transitive closure.

Lemma 7.2. Let $(S, Act, \mathcal{F}, \longrightarrow, \rightsquigarrow, f_0, T)$ be a stochastic automaton. Let $\rho \subseteq S \times S$ be a partial strong stochastic timed bisimulation relation. Then the transitive closure of $\rho \cup \leftrightarrows_{dt}$ is a strong stochastic timed bisimulation relation.

Proof. Let R be the transitive closure of $\rho \cup \leftrightarrows_{dt}$. As $\leftrightarrows_{dt}$ is reflexive, R has to be reflexive, too. Furthermore, since both ρ and $\leftrightarrows_{dt}$ are symmetric, R has to be symmetric, too. Transitivity of R is obvious and hence R is an equivalence relation.

We now show that R is also a strong stochastic timed bisimulation relation. Choose arbitrary $(s, s') \in R$. From the definition of transitive closure it follows that

$$u_0 \Box u_1 \Box \cdots \Box u_k, \text{ for some } u_0, \ldots, u_k \in S \text{ such that } u_0 = s \text{ and } u_k = s', \text{ where } \Box \text{ is either } \rho \text{ or } \leftrightarrows_{dt}.$$

Now, we prove by induction for all $0 \leq i \leq k$, that the following properties hold:

1. if $s \xrightarrow{a}_t f$ for some $f \in \mathcal{F}$, then there is a $f' \in \mathcal{F}$ such that $u_i \xrightarrow{a}_t f'$ and for all $X \subseteq S/R$ it holds that $f(\bigcup X) = f'(\bigcup X)$.
2. if $s \rightsquigarrow_t$, then $u_i \rightsquigarrow_t$.
3. if $s \in T$, then $u_i \in T$.

Note that using symmetry, it follows directly from these properties that R is a strong stochastic timed bisimulation. Properties 2 and 3 follow straightforwardly from the definitions of ρ and $\leftrightarrows_{dt}$. We concentrate on property 1.

For u_0 we have $u_0 = s$ and therefore $s \leftrightarrows_{dt} u_0$. From lemma 6.6 we have that if $s \xrightarrow{a}_t f$, then there is some f' such that $u_0 \xrightarrow{a}_t f'$ and for all $X \subseteq S/_{\leftrightarrows_{dt}}$ it is the case that $f(\bigcup X) = f'(\bigcup X)$. As $\leftrightarrows_{dt} \subseteq R$, and $\leftrightarrows_{dt}$ and R are equivalences, lemma 6.4 yields that for all $X \subseteq S/R$ it holds that $f(\bigcup X) = f'(\bigcup X)$.

Now suppose that properties 1 holds for all $u_0, \ldots, u_i$. We show that it holds for u_{i+1}. There are two cases to consider. Either $u_i \rho u_{i+1}$ or $u_i \underline{\leftrightarrow}_{dt}\ u_{i+1}$.

If $u_i \underline{\leftrightarrow}_{dt}\ u_{i+1}$, then from lemma 6.6 we have if $u_i \xrightarrow{a}_t f'$, then there is some f'' such that $u_{i+1} \xrightarrow{a}_t f''$ and for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it holds that $f'(\bigcup X) = f''(\bigcup X)$. As $\underline{\leftrightarrow}_{dt} \subseteq R$, and both are equivalences, lemma 6.4 yields that forall $X \subseteq S/R$ it is the case that $f'(\bigcup X) = f''(\bigcup X)$.

If $u_i \rho u_{i+1}$ then from the definition of partial strong stochastic bisimulation there is some f'' such that $u_{i+1} \xrightarrow{a}_t f''$ and as $\rho \subseteq R$, it follows using lemma 6.4 that for all $X \subseteq S/R$ it holds that $f'(\bigcup X) = f''(\bigcup X)$.

Together we have $f(\bigcup X) = f'(\bigcup X) = f''(\bigcup X)$ for all $X \subseteq S/R$. Therefore, property number 1 holds. □

Theorem 7.3. Strong stochastic timed bisimulation equivalence is a congruence for the at ($p{}^{c}t$) operator.

Proof. Let $u \in \mathbb{R}^{\geq 0}$. Define $\rho = \{(p{}^{c}u, q{}^{c}u) \mid p \underline{\leftrightarrow}_{dt} q\}$ and let R be the transitive closure of $\rho \cup \underline{\leftrightarrow}_{dt}$. Choose arbitrary $(p{}^{c}u, q{}^{c}u) \in \rho$.

1. If $p{}^{c}u \xrightarrow{a}_t f$, then $p \xrightarrow{a}_t f$ and $t = u$. As $p \underline{\leftrightarrow}_{dt} q$, there must be some $g \in \mathcal{F}$ such that $q \xrightarrow{a}_t g$ and $f(\bigcup X) = g(\bigcup X)$ for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$. As $t = u$, also $q{}^{c}u \xrightarrow{a}_t g$.

   From lemma 6.4 it follows that $f(\bigcup Y) = g(\bigcup Y)$ for all $Y \subseteq S/R$.

2. If $p{}^{c}u \rightsquigarrow_t$, then $t \leq u$ and $p \rightsquigarrow_t$. As $p \underline{\leftrightarrow}_{dt} q$, also $q \rightsquigarrow_t$ and hence (as $t \leq u$) $q{}^{c}u \rightsquigarrow_t$.

3. It is never the case, that $p{}^{c}u \in T$.

Therefore ρ is a partial strong stochastic timed bisimulation and from lemma 7.2 it follows that the transitive closure of $\rho \cup \underline{\leftrightarrow}_{dt}$ is a strong stochastic timed bisimulation relation. Hence, strong stochastic timed bisimulation equivalence is a congruence for the ^{c} operator.

□

Theorem 7.4. Strong stochastic timed bisimulation equivalence is a congruence for the $\gg$ operator.

Proof. Let $u \in \mathbb{R}^{\geq 0}$. Define $\rho = \{(u \gg p, u \gg q) \mid p \underline{\leftrightarrow}_{dt}\ q\}$ and let R be the transitive closure of $\rho \cup \underline{\leftrightarrow}_{dt}$. Choose arbitrary $(u \gg p, u \gg q) \in \rho$. If $u \gg p \xrightarrow{a}_t f$, then $u \leq t$ and $p \xrightarrow{a}_t f$. Because $p \underline{\leftrightarrow}_{dt} q$, we have $q \xrightarrow{a}_t g$ and also $u \gg q \xrightarrow{a}_t g$, where for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it holds that $f(\bigcup X) = g(\bigcup X)$. From lemma 6.4 it follows that $f(\bigcup Y) = g(\bigcup Y)$ for all $Y \subseteq S/R$.

Furthermore $u \gg p \rightsquigarrow_t$ means that either $t < u$ and therefore $u \gg q \rightsquigarrow_t$, or $p \rightsquigarrow_t$ and therefore $q \rightsquigarrow_t$ and hence also $u \gg q \rightsquigarrow_t$. Finally, note that it is never the case that $t \gg p \in T$.

Therefore, ρ is a partial strong stochastic timed bisimulation and from lemma 7.2 it follows that R is a strong stochastic timed bisimulation relation. Hence, strong stochastic timed bisimulation equivalence is a congruence for the $\gg$ operator. □

Theorem 7.5. Strong stochastic timed bisimulation equivalence is a congruence for the encapsulation (∂_H) operator.

Proof. Let $H \subseteq \mathit{Act}$ be a set of action labels. Define $R = \{(\partial_H(p), \partial_H(q)) \mid p \underline{\leftrightarrow}_{dt} q\} \cup \{(p, p) \mid p \in S\}$. Choose arbitrary $(p_1, q_1) \in R$. The case when $p_1 = q_1$ is trivial, therefore it is sufficient to consider only the case when $p_1 = \partial_H(p)$ and $q_1 = \partial_H(q)$ for some $p, q \in \mathbb{P}_{det}$ such that $p \underline{\leftrightarrow}_{dt}\ q$.

If $\partial_H(p) \xrightarrow{a}_t f$, then $a \notin H$ and $p \xrightarrow{a}_t f'$ where $f = \lambda U{:}2^S.f'(\{r | \partial_H(r) \in U\})$. As $p \underline{\leftrightarrow}_{dt} q$, it follows that $q \xrightarrow{a}_t g'$ such that for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it holds $f'(\bigcup X) = g'(\bigcup X)$. Consequently, $\partial_H(q) \xrightarrow{a}_t g$ where $g = \lambda U{:}2^S.g'(\{r | \partial_H(r) \in U\})$.

Let $Y \subseteq S/R$. Now denote $V = \{r \mid \partial_H(r) \in Y\}$. We show that V is closed under $\underline{\leftrightarrow}_{dt}$. Let $u \underline{\leftrightarrow}_{dt} u'$ and $u \in V$. Then $\partial_H(u) \in Y$. As $(\partial_H(u), \partial_H(u')) \in R$ it follows that $\partial_H(u') \in Y$ and therefore, $u' \in V$. Hence $V \subseteq S/_{\underline{\leftrightarrow}_{dt}}$. Thus

$$f(Y) = f'(V) = g'(V) = g(Y).$$

Moreover, if $\partial_H(p) \rightsquigarrow_t$, then $p \rightsquigarrow_t$. As $p \underline{\leftrightarrow}_{dt}\, q$ also $q \rightsquigarrow_t$ and therefore $\partial_H(q) \rightsquigarrow_t$.

Finally, it is never the case that $\partial_H(p) \in T$. Therefore, R is a strong stochastic timed bisimulation. Hence, strong stochastic timed bisimulation is a congruence for the encapsulation operator. □

Theorem 7.6. Strong stochastic timed bisimulation equivalence is a congruence for the $+$ operator.

Proof. Define the relation $\rho = \{(p{+}q, p'{+}q') \mid p\underline{\leftrightarrow}_{dt}p', q\underline{\leftrightarrow}_{dt}q'\}$ and let R be the transitive closure of $\rho \cup \underline{\leftrightarrow}_{dt}$. Note that ρ is an equivalence relation, which follows because $\underline{\leftrightarrow}_{dt}$ is an equivalence relation. Also, R is an equivalence relation, as both ρ and $\underline{\leftrightarrow}_{dt}$ are equivalence relations.

Choose arbitrary $(p, q) \in \rho$. Hence, $p = p_1 + p_2$ and $q = q_1 + q_2$, where $p_1\underline{\leftrightarrow}_{dt}q_1$ and $p_2\underline{\leftrightarrow}_{dt}q_2$. If $p \xrightarrow{a}_t f$ then either $p_1 \xrightarrow{a}_t f$ or $p_2 \xrightarrow{a}_t f$ (following the operational rules). Because both situations are symmetric we can without loss of generality consider only the first one.

From $p_1\underline{\leftrightarrow}_{dt}q_1$ and lemma 6.6, it follows that there is some f' such that $q_1 \xrightarrow{a}_t f'$ and for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it is the case that $f(\bigcup X) = f'(\bigcup X)$. As $\underline{\leftrightarrow}_{dt} \subseteq R$, we have from lemma 6.4 that for all $Y \subseteq S/R$ it is the case that $f(\bigcup Y) = f'(\bigcup Y)$. Because $q = q_1{+}q_2$, it holds $q \xrightarrow{a}_t f'$.

Furthemore if $p \rightsquigarrow_t$, then either $p_1 \rightsquigarrow_t$ or $p_2 \rightsquigarrow_t$. From $p_1\underline{\leftrightarrow}_{dt}q_1$ (or $p_2\underline{\leftrightarrow}_{dt}q_2$)) we have $q_1 \rightsquigarrow_t$ (or $q_2 \rightsquigarrow_t$). Therefore, $q \rightsquigarrow_t$. Because $p = p_1{+}p_2$, it is never the case that $p \in T$.

Therefore ρ is partial strong stochastic timed bisimulation and from lemma 7.2 it follows that R is a strong stochastic timed bisimulation relation. As all pairs of processes $(p{+}q, p'{+}q')$ such that $p\underline{\leftrightarrow}_{dt}p'$ and $q\underline{\leftrightarrow}_{dt}q'$ are in R, it follows that $p{+}q\underline{\leftrightarrow}_{dt}p'{+}q'$. Therefore, $\underline{\leftrightarrow}_{dt}$ is a congruence for $+$. □

Theorem 7.7. Strong stochastic timed bisimulation equivalence is a congruence for the $\|$ operator.

Proof. We define the relation $\rho = \{(p\|q, p'\|q') \mid p\underline{\leftrightarrow}_{dt}p', q\underline{\leftrightarrow}_{dt}\, q'\}$. The relation ρ is symmetric and transitive, as $\underline{\leftrightarrow}_{dt}$ is symmetric and transitive.

Let $(p, q) \in \rho$. Then $p = p_1\|p_2$ and $q = q_1\|q_2$ for some $p_1, p_2, q_1, q_2 \in S$ such that $p_1\underline{\leftrightarrow}_{dt}q_1$ and $p_2\underline{\leftrightarrow}_{dt}q_2$. If $p_1\|p_2 \xrightarrow{a}_t f_p$, then either

1. $f_p = \mathit{Stoch}(t{\gg}p_2)$, $p_1 \xrightarrow{a}_t f_\checkmark$ and $p_2 \rightsquigarrow_t$ or $f_p = \mathit{Stoch}(t{\gg}p_1)$, $p_2 \xrightarrow{a}_t f_\checkmark$ and $p_1 \rightsquigarrow_t$, which is the symmetric situation. Without loss of generality, we only consider the first case.

   As $p_1\underline{\leftrightarrow}_{dt}q_1$, $q_1 \xrightarrow{a}_t f_\checkmark$ (using lemma 6.7) and as $p_2\underline{\leftrightarrow}_{dt}q_2$, $q_2 \rightsquigarrow_t$. It follows that $q_1\|q_2 \xrightarrow{a}_t \mathit{Stoch}(t{\gg}q_2)$. As $\underline{\leftrightarrow}$ is a congruence for $\gg$ (see corollary 7.10; we carefully checked that there are no circular dependencies in proofs), we have

   $$f_p(\bigcup X) = \mathit{Stoch}(t{\gg}p_2)(\bigcup X) = \mathit{Stoch}(t{\gg}q_2)(\bigcup X) \text{ for all } X \subseteq S/_{\underline{\leftrightarrow}_{dt}}.$$

   Therefore, using lemma 6.4, it follows that

   $$f_p(\bigcup X) = \mathit{Stoch}(t{\gg}p_2)(\bigcup X) = \mathit{Stoch}(t{\gg}q_2)(\bigcup X) \text{ for all } X \subseteq S/_{(\rho\cup\underline{\leftrightarrow}_{dt})^*},$$

   where $(\rho \cup \underline{\leftrightarrow}_{dt})^*$ denotes the transitive closure of $\rho \cup \underline{\leftrightarrow}_{dt}$ (see definition 7.1).

2. There is some $f_{p_1} \in \mathcal{F}$ such that $p_1 \xrightarrow{a}_t f_{p_1}$, $f_{p_1} \neq f_\checkmark$ and $f_p(U) = f_{p_1}(\{r|(r\|t{\gg}p_2) \in U\})$ and $p_2 \rightsquigarrow_t$. It may be the case that $f_{p_2} \in \mathcal{F}$ such that $p_2 \xrightarrow{a}_t f_{p_2}$ and $f_p(U) = f_{p_2}(\{r|(t{\gg}p_1\|r) \in U\})$ and $p_1 \rightsquigarrow_t$. This is the symmetric situation; we treat here only the first case.

   As $q_1\underline{\leftrightarrow}_{dt}p_1$ and $q_2\underline{\leftrightarrow}_{dt}p_2$, it follows that $q_2 \rightsquigarrow_t$ and there must be some $f_{q_1} \in \mathcal{F}$ such that $q_1 \xrightarrow{a}_t f_{q_1}$ and

   $$\forall X \subseteq S/_{\underline{\leftrightarrow}_{dt}} : \; f_{p_1}(\bigcup X) = f_{q_1}(\bigcup X).$$

   Hence $q_1\|q_2 \xrightarrow{a}_t f_q$, where $f_q(U) = f_{q_1}(\{r \mid (r\|t{\gg}q_2) \in U\})$.

   Take arbitrary $Y \subseteq S/_{(\rho\cup\underline{\leftrightarrow}_{dt})^*}$. Denote

   $$\alpha_p = \{r \mid (r\|t{\gg}p_2) \in \bigcup Y\} \quad \text{and} \quad \alpha_q = \{r \mid (r\|t{\gg}q_2) \in \bigcup Y\}.$$

   Now we are going to prove, that $\alpha_p = \alpha_q$ and that α_p (and hence also α_q) is a composition of equivalence classes from $S/_{\underline{\leftrightarrow}_{dt}}$.

- if $r \in \alpha_p$, then $(r\|t{\gg}p_2) \in \bigcup Y$. Thus $(r\|t{\gg}p_2, r\|t{\gg}q_2) \in \rho$ (as $r\underline{\leftrightarrow}_{dt}r$ and (from lemma 7.4) $t{\gg}p_2\underline{\leftrightarrow}_{dt}t{\gg}q_2$). Hence, $(r\|t{\gg}q_2) \in \bigcup Y$ and therefore $r \in \alpha_q$. The other inclusion can be proven analogically. Therefore $\alpha_p = \alpha_q$.
- Suppose $r \in \alpha_p$ and $r' \notin \alpha_p$, for some $r, r' \in S$. Then $(r\|t{\gg}p_2) \in \bigcup Y$ and $(r'\|t{\gg}p_2) \notin \bigcup Y$. If $r\underline{\leftrightarrow}_{dt}r'$, then, as $t{\gg}p_2\underline{\leftrightarrow}_{dt}t{\gg}p_2$, it follows that $(r\|t{\gg}p_2, r'\|t{\gg}p_2) \in \rho$ and therefore $(r'\|t{\gg}p_2) \in \bigcup Y$. Thus, $r' \in \alpha_p$, which is a contradiction. Hence, $r\not\underline{\leftrightarrow}_{dt}r'$ which means that α_p is closed under $\underline{\leftrightarrow}_{dt}$, therefore $\alpha_p \subseteq S/_{\underline{\leftrightarrow}_{dt}}$.

  Now we have for arbitrary $Y \subseteq S/_{(\rho\cup\underline{\leftrightarrow}_{dt})^*}$

$$f_p(\bigcup Y){=}f_{p_1}(\{r|(r\|t{\gg}p_2){\in}\bigcup Y\}){=}f_{p_1}(\alpha_p){=}f_{q_1}(\alpha_q){=}f_{q_1}(\{r|(r\|t{\gg}q_2){\in}\bigcup Y\}){=}f_q(\bigcup Y).$$

3. There are some $f_{p_1}, f_{p_2} \in \mathcal{F}$ such that $p_1 \xrightarrow{b}_t f_{p_1}$, $p_2 \xrightarrow{c}_t f_{p_2}$, $f_{p_1} \neq f_{\checkmark}$, $f_{p_2} \neq f_{\checkmark}$, $\gamma(b, c) = a$ and $f_p(U) = f_{p_1}(\{r|\exists s.(r\|s) \in U\}){\cdot}f_{p_2}(\{s|\exists r.(r\|s) \in U\})$.

   As $q_1\underline{\leftrightarrow}_{dt}p_1$ and $q_2\underline{\leftrightarrow}_{dt}p_2$, it follows that there must be some $f_{q_1}, f_{q_2} \in \mathcal{F}$ such that

$$q_1 \xrightarrow{a}_t f_{q_1} \text{ and } \forall X \subseteq S/_{\underline{\leftrightarrow}_{dt}} : \ f_{p_1}(\bigcup X) = f_{q_1}(\bigcup X).$$

$$q_2 \xrightarrow{b}_t f_{q_2} \text{ and } \forall X \subseteq S/_{\underline{\leftrightarrow}_{dt}} : \ f_{p_2}(\bigcup X) = f_{q_2}(\bigcup X).$$

   Hence $q_1\|q_2 \xrightarrow{a}_t f_q$, where $f_q(U) = f_{q_1}(\{r|\exists s.(r\|s) \in U\}){\cdot}f_{q_2}(\{s|\exists r.(r\|s) \in U\})$. Take arbitrary $Y \subseteq S/_{(\rho\cup\underline{\leftrightarrow}_{dt})^*}$. Denote

$$\alpha_p = \{r|\exists s.(r\|s) \in \bigcup Y\} \quad \text{and} \quad \alpha_q = \{s|\exists r.(r\|s) \in \bigcup Y\}.$$

   Suppose $r \in \alpha_p$ and $r' \notin \alpha_p$ for some $r, r' \in S$. Then, there is some $s \in S$ such that $r\|s \in \bigcup Y$ and for all $t \in S$ it holds that $r'\|t \notin \bigcup Y$. If $r \underline{\leftrightarrow}_{dt} r'$, then $(r\|s, r'\|s) \in \rho$ and therefore $(r'\|s) \in \bigcup Y$, which is a contradiction. Hence, $r \not\underline{\leftrightarrow}_{dt} r'$. Thus α_p is closed under stochastic timed bisimulation, which means that $\alpha_p \subseteq S/_{\underline{\leftrightarrow}_{dt}}$. Analogically, we can prove that $\alpha_q \subseteq S/_{\underline{\leftrightarrow}_{dt}}$.

   Now we can see that

$$f_p(\bigcup Y) = f_{p_1}(\alpha_p){\cdot}f_{p_2}(\alpha_q) = f_{q_1}(\alpha_p){\cdot}f_{q_2}(\alpha_q) = f_q(\bigcup Y).$$

4. There are some $b, c \in \mathit{Act}$ such that $\gamma(b, c) = a$ and $p_1 \xrightarrow{b}_t f_p$, $p_2 \xrightarrow{c}_t f_{\checkmark}$ or $p_1 \xrightarrow{b}_t f_{\checkmark}$, $p_2 \xrightarrow{c}_t f_p$. As both cases are symmetric we only consider the first case without loss of generality.

   As $p_1 \underline{\leftrightarrow}_{dt} q_1$, it follows that $q_1 \xrightarrow{b}_t f_q$ such that for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it holds that $f_p(\bigcup X) = f_q(\bigcup X)$. Also, as $p_2 \underline{\leftrightarrow}_{dt} q_2$ from lemma 6.7 it follows that $q_2 \xrightarrow{c}_t f_{\checkmark}$. Therefore $q_1 \parallel q_2 \xrightarrow{a}_t f_q$ and from lemma 6.4 we have that

$$f_p(\bigcup X) = f_q(\bigcup X) \text{ for all } X \subseteq S/_{(\rho\cup\underline{\leftrightarrow}_{dt})^*}.$$

5. There are some $b, c \in \mathit{Act}$ such that $\gamma(b, c) = a$, $p_1 \xrightarrow{b}_t f_{\checkmark}$ and $p_2 \xrightarrow{c}_t f_{\checkmark}$. From lemma 6.7, using the fact that $p_1 \underline{\leftrightarrow}_{dt} q_1$ and $p_2 \underline{\leftrightarrow}_{dt} q_2$, it follows that $q_1 \xrightarrow{b}_t f_{\checkmark}$ and $q_2 \xrightarrow{c}_t f_{\checkmark}$. Therefore $q_1 \parallel q_2 \xrightarrow{a}_t f_{\checkmark}$.

Furthermore, if $p_1\|p_2 \rightsquigarrow_t$, then $p_1 \rightsquigarrow_t$ and $p_2 \rightsquigarrow_t$ and as $p_1\underline{\leftrightarrow}_{dt}q_1, p_2\underline{\leftrightarrow}_{dt}q_2$, also $q_1\|q_2 \rightsquigarrow_t$.

Finally, it is never the case that $p_1\|p_2 \in T$. Therefore ρ is a partial strong stochastic timed bisimulation. Hence, from the lemma 7.2 follows that $(\rho \cup \underline{\leftrightarrow}_{dt})^*$ is a strong stochastic timed bisimulation relation and therefore $\underline{\leftrightarrow}_{dt}$ is a congruence for the $\|$ operator. □

Theorem 7.8. Strong stochastic timed bisimulation equivalence is a congruence for the $b{\rightarrow}\_{\diamond}\_$ operator.

Proof. Let b be a fixed boolean condition. Define the relation $\rho = \{(b \rightarrow p \diamond q, b \rightarrow p' \diamond q') \mid p \leftrightarroweq_{dt} p', q \leftrightarroweq_{dt} q'\}$. The relation ρ is symmetric and transitive due to the fact that $\leftrightarroweq_{dt}$ is symmetric and transitive.

Let $(p, q) \in \rho$. Then $p = b \rightarrow p_1 \diamond p_2$ and $q = b \rightarrow q_1 \diamond q_2$ for some $p_1, p_2, q_1, q_2 \in S$ such that $p_1 \leftrightarroweq_{dt} q_1$ and $p_2 \leftrightarroweq_{dt} q_2$.

1. Suppose $p \xrightarrow{a}_t f$, then either

   - $b = \mathit{true}$ and $p_1 \xrightarrow{a}_t f$. Hence, there is some $g \in \mathcal{F}$ such that $q_1 \xrightarrow{a}_t g$ and for all $X \subseteq S/_{\leftrightarroweq_{dt}}$ it holds $f(\bigcup X) = g(\bigcup X)$. Therefore $q \xrightarrow{a}_t g$.

   or

   - $b = \mathit{false}$ and $p_2 \xrightarrow{a}_t f$. In this case there is some $g \in \mathcal{F}$ such that $q_2 \xrightarrow{a}_t g$ and for all $X \subseteq S/_{\leftrightarroweq_{dt}}$ it holds that $f(\bigcup X) = g(\bigcup X)$. Therefore, $q \xrightarrow{a}_t g$.

2. Suppose $p \leadsto_t$, then either

   - $b = \mathit{true}$ and $p_1 \leadsto_t$. So, $q_1 \leadsto_t$ and therefore $q \leadsto_t$.

   or

   - $b = \mathit{false}$ and $p_2 \leadsto_t$. Clearly, $q_2 \leadsto_t$ and therefore $q \leadsto_t$.

3. As $p = b \rightarrow p_1 \diamond p_2$, it is never the case that $p \in T$.

Therefore, ρ is a partial strong stochastic timed bisimulation. Hence, from lemma 7.2 it follows that $(\rho \cup \leftrightarroweq_{dt})^*$ is a strong stochastic timed bisimulation relation and therefore $\leftrightarroweq_{dt}$ is a congruence for the $b \rightarrow \_ \diamond \_$ operator. □

Theorem 7.9. Let $\mathcal{OP} : \mathbb{P} \rightarrow \mathbb{P}$ be a unary process operator such that strong stochastic timed bisimulation equivalence is a congruence for $\mathcal{OP}$ and the following properties hold

- $\mathit{stochvar}(\mathcal{OP}(p)) = \mathit{stochvar}(p)$,
- $[\![\mathcal{OP}(p)]\!] = [\![p]\!]$, and
- $\mathit{det}(\mathcal{OP}(p)) = \mathcal{OP}(\mathit{det}(p))$.

Then general stochastic bisimulation is a congruence for the operator $\mathcal{OP}$.

Proof. Let p, q be arbitrary processes such that $p \leftrightarroweq q$. We show that $\mathcal{OP}(p) \leftrightarroweq \mathcal{OP}(q)$. Let X be a subset of $S/_{\leftrightarroweq_{dt}}$. Define the set

$$Y = \{r \in \mathbb{P}_{det} \mid \mathcal{OP}(r) \in \bigcup X\}.$$

There are three observations that we use about Y.

1. The set $\mathcal{D}_p(Y)$ is a measurable set. This follows because $\mathcal{D}_{\mathcal{OP}(p)}(\bigcup X)$ is a measurable set and $\mathcal{D}_p(Y) = \mathcal{D}_{\mathcal{OP}(p)}(\bigcup X)$. This last observation can be seen as follows:

$$\begin{array}{rcl} \mathcal{D}_p(Y) & = & \{d \in \mathit{stochvar}(p) \mid \mathit{det}(p)(d) \in Y\} \\ & = & \{d \in \mathit{stochvar}(p) \mid \mathcal{OP}(\mathit{det}(p))(d) \in \bigcup X\} \\ & = & \{d \in \mathit{stochvar}(p) \mid \mathit{det}(\mathcal{OP}(p))(d) \in \bigcup X\} \\ & = & \mathcal{D}_{\mathcal{OP}(p)}(\bigcup X) \end{array}$$

2. The set $\mathcal{D}_q(Y)$ is a measurable set. This follows as $\mathcal{D}_q(Y) = \mathcal{D}_{\mathcal{OP}(q)}(\bigcup X)$, which can be proven in exactly the same way as the observation in the previous item.

3. The set Y is bisimulation closed, i.e., if $r \leftrightarroweq_{dt} r'$, then $r \in Y$ iff $r' \in Y$. We prove this as follows. Assume that $r \in Y$. Then $\mathcal{OP}(r) \in \bigcup X$. As $r \leftrightarroweq_{rt} r'$, $\leftrightarroweq_{rt}$ is a congruence for $\mathcal{OP}$ and $\bigcup X$ is bisimulation closed, $\mathcal{OP}(r') \in \bigcup X$. So, $r' \in Y$.

Using these observations we can derive

$$
\begin{aligned}
&\mathit{Stoch}(\mathcal{OP}(p))(\textstyle\bigcup X) = \\
&\qquad\qquad \int_{\mathcal{D}_{\mathcal{OP}(p)}(\bigcup X)} [\![\mathcal{OP}(p)]\!] d\mu_{stochvar(\mathcal{OP}(p))} = \\
&\qquad\qquad \int_{\mathcal{D}_p(Y)} [\![p]\!] d\mu_{stochvar(p)} = \\
&\qquad\qquad \mathit{Stoch}(p)(Y) = \qquad (Y \text{ is a measurable set and bisimulation closed, } p\underline{\leftrightarrow}q) \\
&\qquad\qquad \mathit{Stoch}(q)(Y) = \\
&\qquad\qquad \int_{\mathcal{D}_q(Y_p)} [\![q]\!] d\mu_{stochvar(q)} = \\
&\qquad\qquad \int_{\mathcal{D}_{\mathcal{OP}(q)}(\bigcup X)} [\![\mathcal{OP}(q)]\!] d\mu_{stochvar(\mathcal{OP}(q))} = \\
&\qquad\qquad \mathit{Stoch}(\mathcal{OP}(q))(\bigcup X).
\end{aligned}
$$

Finally, suppose that d is possible in $\mathcal{OP}(p)$. Then as $stochvar(p){=}stochvar(\mathcal{OP}(p))$ and $[\![p]\!]{=}[\![\mathcal{OP}(p)]\!]$ it holds that d is also possible in p and therefore (as $p\underline{\leftrightarrow}q$), there exists some e which is possible in q and hence, by the same argument as before, e is also possible in $\mathcal{OP}(q)$. □

Corollary 7.10. General stochastic bisimulation is a congruence for the $\gg$, ∂ and ‹ operators.

Theorem 7.11. Strong stochastic timed bisimulation equivalence is a congruence for the $\cdot$ operator.

Proof. Let R^* be the transitive closure of $\{(p{\cdot}q, p'{\cdot}q') \mid p\underline{\leftrightarrow}_{dt}p', q\underline{\leftrightarrow}q'\}\cup\underline{\leftrightarrow}_{dt}$. Take arbitrary $(p{\cdot}q, p'{\cdot}q') \in R^*$. We only consider the case when $p \underline{\leftrightarrow}_{dt} p'$ and $q \underline{\leftrightarrow} q'$, as the other is trivial.

If $p{\cdot}q \xrightarrow{a}_t f$ then either $f = \lambda U{:}2^S.g(\{r|r{\cdot}q \in U\})$, $g \neq f_{\checkmark}$ and $p \xrightarrow{a}_t g$, or $f = \mathit{Stoch}(t{\gg}q)$ and $p \xrightarrow{a}_t f_{\checkmark}$. We consider both cases separately.

1. In the first case, as $p \underline{\leftrightarrow}_{dt} p'$ we have $p' \xrightarrow{a}_t g'$ such that for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it holds that $g(\bigcup X) = g'(\bigcup X)$. Hence $p'{\cdot}q' \xrightarrow{a}_t f'$ where $f' = \lambda U{:}2^S.g'(\{r|r{\cdot}q' \in U\})$.

   Now, denote $K_U = \{r \mid r{\cdot}q \in U\}$ and $K'_U = \{r \mid r{\cdot}q' \in U\}$. We show that $K_Y = K'_Y$ for all $Y{\in}2^S/_{R^*}$. If $r \in K_Y$, then $r{\cdot}q \in Y$. As $r\underline{\leftrightarrow}_{dt}r$ and $q\underline{\leftrightarrow}q'$, it follows that $r{\cdot}q' \in Y$ and thus, $r \in K'_Y$. As this is symmetric, we have $K_Y = K'_Y$.

   Furthermore, we prove that every K_Y where $Y{\in}S/_{R^*}$, is a union of some equivalence classes from $S/_{\underline{\leftrightarrow}_{dt}}$, i.e., for all $X \in S/_{\underline{\leftrightarrow}_{dt}}$, if $X \cap K_Y \neq \emptyset$ then $X \subseteq K_Y$. Suppose $x \in X \cap K_Y$ and choose arbitrary $y \in X$. Then, it follows that $x{\cdot}q \in Y$ and as $x\underline{\leftrightarrow}_{dt}y$ and $q\underline{\leftrightarrow}q$, we have that $x{\cdot}qR^*y{\cdot}q$ and hence $y{\cdot}q \in Y$. So, $y \in K_Y$ and therefore $X \subseteq K_Y$.

   Using these two facts and the equivalence of g and g' on the equivalence classes from $S/_{\underline{\leftrightarrow}_{dt}}$, we have for every $X{\subseteq}S/_{R^*}$:

   $$f(\bigcup X) = g(K_{\bigcup X}) = g(\bigcup_{Y\in X} K_Y) = g'(\bigcup_{Y\in X} K_Y) = g'(K_{\bigcup X}) = g'(K'_{\bigcup X}) = f'(\bigcup X).$$

2. In the second case $f = \mathit{Stoch}(t{\gg}q)$ and $p \xrightarrow{a}_t f_{\checkmark}$. As $p \underline{\leftrightarrow}_{dt} p'$ we have $p' \xrightarrow{a}_t f_{\checkmark}$ and therefore $p'{\cdot}q' \xrightarrow{a}_t \mathit{Stoch}(t{\gg}q')$. As $q \underline{\leftrightarrow} q'$, it follows from corollary 7.10 that for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$:

   $$f(\bigcup X) = \mathit{Stoch}(t{\gg}q)(\bigcup X) = \mathit{Stoch}(t{\gg}q')(\bigcup X) = f'(\bigcup X).$$

It is left to check that terminating states and the idle relation are properly mimicked. As this is straightforward this is omitted (see e.g., the proof of theorem 7.6). □

The following auxiliary definition is used to identify subsets of data which cause the same behaviour in a process p. For sets of processes the meaning of *closed under bisimulation* is standard as bisimulation is defined on processes.

Definition 7.12. Let p be an arbitrary process and $D = \mathit{stochvar}(p)$. We say that $D' \subseteq D$ is *closed under bisimulation* (w.r.t. p) iff for all $d \in D'$ and $d' \in D \setminus D'$, it holds that $\mathit{det}(p)(d) \not\leftrightarrow_{dt} \mathit{det}(p)(d')$.

Lemma 7.13. Let p and q be processes. Let $D = \mathit{stochvar}(p)$ and $E = \mathit{stochvar}(q)$. Furthermore, let $\{(D_i, E_i)\}_{i=1}^{N}$ be a finite sequence of measurable rectangles from $D \times E$ in the sense that for every $1 \leq i \leq N$, it holds that $D_i \subseteq D$ and $E_i \subseteq E$. Then a finite, disjoint sequence $\{(D_i^*, E_i^*)\}_{i=1}^{M}$ of measurable rectangles from $D \times E$ exists such that

$$\bigcup_{i=1}^{M}(D_i^* \times E_i^*) = \bigcup_{i=1}^{N}(D_i \times E_i),$$

where disjoint means that for every $i \neq j$: $(D_i^* \times E_i^*) \cap (D_j^* \times E_j^*) = \emptyset$.

Furthermore, if all D_i are closed under bisimulation, then all D_i^* are closed under bisimulation, too, and if all E_i are closed under bisimulation, then also all E_i^* are closed under bisimulation.

Proof. We construct the desired sequence R by the following algorithm:

- Initialize $R := \{(D_i, E_i)\}_1^N$.
- If there are pairs $(\tilde{D}_i, \tilde{E}_i)$ and $(\tilde{D}_j, \tilde{E}_j) \in R$ such that $(\tilde{D}_i \times \tilde{E}_i) \cap (\tilde{D}_j \times \tilde{E}_j) \neq \emptyset$, then remove $(\tilde{D}_i, \tilde{E}_i), (\tilde{D}_j, \tilde{E}_j)$ from R and add the following seven pairs to R. We only us intersection and set subtraction, which means that the resulting sets are still measurable.

$$\begin{array}{l}(\tilde{D}_j \setminus \tilde{D}_i, \tilde{E}_i \cap \tilde{E}_j),\\ (\tilde{D}_j \setminus \tilde{D}_i, \tilde{E}_j \setminus \tilde{E}_i),\\ (\tilde{D}_i \cap \tilde{D}_j, \tilde{E}_i \setminus \tilde{E}_j),\\ (\tilde{D}_i \cap \tilde{D}_j, \tilde{E}_i \cap \tilde{E}_j),\\ (\tilde{D}_i \cap \tilde{D}_j, \tilde{E}_j \setminus \tilde{E}_i),\\ (\tilde{D}_i \setminus \tilde{D}_j, \tilde{E}_i \setminus \tilde{E}_j),\\ (\tilde{D}_i \setminus \tilde{D}_j, \tilde{E}_i \cap \tilde{E}_j).\end{array}$$

  This step is repeated as long as there are pairs in R with overlapping elements.

Note that the union of the products of the new sets match exactly $(\tilde{D}_i \times \tilde{E}_i) \cup (\tilde{D}_j \times \tilde{E}_j)$. Therefore, it is straightforward to see that

$$\bigcup_{i=1}^{M}(D_i^* \times E_i^*) = \bigcup_{i=1}^{N}(D_i \times E_i)$$

holds during each iteration of the algorithm.

In order to see that this algorithm terminates, one can consider the set of all minimal sets H_D obtained by closing $\{D_i \mid 1 \leq i \leq N\}$ under intersection and removing every set for which there is a strict subset. In the same way H_E can be obtained from $\{E_i \mid 1 \leq i \leq N\}$. Define $\mathit{count}(D, E)$ as the number of pairs of sets $\hat{D} \times \hat{E}$ with $\hat{D} \in H_D$ and $\hat{E} \in H_E$ such that $\hat{D} \times \hat{E} \subseteq D \times E$. The measure

$$\sum_{(D,E) \in R} \mathit{count}(D, E)$$

decreases by at least one with every step of the algorithm.

Finally, we need to show that for every $(\tilde{D}_j, \tilde{E}_j)$ added to R during each iteration, $\tilde{D}_j$ is closed under bisimulation, provided that for each $(\tilde{D}_i, \tilde{E}_i)$ which was in R before the iteration it holds that $\tilde{D}_i$ is closed under bisimulation. This also needs to be shown for $\tilde{E}_i$, but that argument is exactly the same, and therefore skipped.

First, consider the case where a pair $(\tilde{D}_i \cap \tilde{D}_j, \ldots)$ is added to R. Consider a $d \in \tilde{D}_i \cap \tilde{D}_j$ and a $d' \notin \tilde{D}_i \cap \tilde{D}_j$. So, $d \in \tilde{D}_i$ and $d \in \tilde{D}_j$, whereas $d' \notin \tilde{D}_i$ or $d' \notin \tilde{D}_j$. Therefore, $det(p)(d) \not\underline{\leftrightarrow}_{dt} det(p)(d')$.

Secondly, consider the case where a pair $(\tilde{D}_i \setminus \tilde{D}_j, \ldots)$ is added to R. Consider a $d \in \tilde{D}_i \setminus \tilde{D}_j$ and a $d' \notin \tilde{D}_i \setminus \tilde{D}_j$. So, $d \in \tilde{D}_i$ and $d \notin \tilde{D}_j$, whereas $d' \notin \tilde{D}_i$ or $d' \in \tilde{D}_j$. Also in this case it follows that $det(p)(d) \not\underline{\leftrightarrow}_{dt} det(p)(d')$, which finishes the proof. □

Theorem 7.14. Let $\mathcal{A}$ be a measurable data algebra and assume that all process expressions are bisimulation resilient wrt. $\mathcal{A}$. Then general stochastic bisimulation is a congruence for the stochastic operator.

Proof. Consider two process expressions p and p' containing a free variable $d \in D$ such that $p(d) \underline{\leftrightarrow} p'(d)$ for all $d \in D$ (in short $p \underline{\leftrightarrow} p'$). We must show that $\frac{f}{d{:}D} p \;\underline{\leftrightarrow}\; \frac{f}{d{:}D} p'$.

We first prove the second property of general stochastic bisimulation as it is almost trivial, and substantially easier than the first part. For the second property, we must show that for all possible e in $\frac{f}{d{:}D} p$ there is a possible e' in $\frac{f}{d{:}D} p'$ such that $det(\frac{f}{d{:}D} p)(e) \;\underline{\leftrightarrow}_{dt}\; det(\frac{f}{d{:}D} p')(e')$. This means that e has the shape (e_1, e_2) and e_2 is possible in p and the integral of f over every environment around e_1 is greater than zero. As $p \;\underline{\leftrightarrow}\; p'$, there exists some e_2' possible in p' such that $det(p)(e_2) \;\underline{\leftrightarrow}_{dt}\; det(p')(e_2')$. By definition 4.3 $det(\frac{f}{d{:}D} p)(e) = det(p)(e_2)$ and $det(\frac{f}{d{:}D} p')(e') = det(p')(e_2')$. So, it follows that $det(\frac{f}{d{:}D} p)(e) \;\underline{\leftrightarrow}_{dt}\; det(\frac{f}{d{:}D} p')(e')$.

In the first part of the proof we must show that for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it is the case that $Stoch(\frac{f}{d{:}D} p)(\bigcup X) = Stoch(\frac{f}{d{:}D} p')(\bigcup X)$. As all processes are bisimulation resilient, we find that

$$\begin{aligned}
Stoch(\tfrac{f}{d{:}D} p)(\textstyle\bigcup X) &\overset{\text{Def. 5.6}}{=} \int_{\mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)} [\![\frac{f}{d{:}D} p]\!] d\mu_{D \times stochvar(p)} \\
&\overset{\text{Def. 5.4}}{=} \int_{(e_1, e_2) \in \mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)} f(e_1) \cdot [\![p(e_1)]\!](e_2) d\mu_{D \times stochvar(p)} \qquad (7.1) \\
&\overset{\text{Cor. 3.16}}{=} Sup \left\{ \sum_{i=1}^{N} \left(\int_{a \in A_i} f(a) \cdot \int_{b \in B_i} [\![p(a)]\!](b) d\mu_{stochvar(p)} d\mu_D \right) \right\}
\end{aligned}$$

where the supremum is taken over all possible sequences $\{A_i, B_i\}_1^N$ such that A_i, B_i are measurable, $\bigcup_{i=1}^N A_i \times B_i \subseteq \mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)$ and $A_i \times B_i$ are pairwise disjoint. However, we need that the B_i are closed under bisimulation, i.e., for all $d \in D$, $e \in B_i$ and $e' \in B \backslash B_i$ it holds that $det(p)(d, e) \not\underline{\leftrightarrow}_{dt} det(q)(d, e')$.

First we show that there is a sequence of not necessarily disjoint rectangular sets $\{(A_i, B_i')\}_1^N$ such that all B_i are closed under bisimulation and

$$\bigcup_{i=1}^{N} A_i \times B_i \subseteq \bigcup_{i=1}^{N} A_i \times B_i' \subseteq \mathcal{D}_{\frac{f}{d:D} p}(\bigcup X). \qquad (7.2)$$

The sets B_i' are constructed as the closure under bisimulation of B_i:

$$B_i' = \mathcal{D}_q(\{r | \forall d \in D, \exists e \in B_i . r \;\underline{\leftrightarrow}_{dt}\; det(p)(d, e)\}).$$

Note that as processes are bisimulation resilient, the sets B_i' are measurable. As $B_i \subseteq B_i'$, the subset relation at the left of (7.2) holds trivially. For the right subset relation consider a pair $(a, b') \in A_i \times B_i'$. Then there must be some $(a, b) \in A_i \times B_i \subseteq \mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)$ such that $det(p)(a, b) \;\underline{\leftrightarrow}_{dt}\; det(p)(a, b')$ and as $\mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)$ is closed under bisimulation, $(a, b') \in \mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)$. Therefore every $A_i \times B_i'$ is a subset of $\mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)$ and thus the union $\bigcup_{i=1}^N A_i \times B_i'$ also has to be a subset of $\mathcal{D}_{\frac{f}{d:D} p}(\bigcup X)$.

Given the sequence $\{A_i, B'_i\}_1^N$, we know using lemma 7.13 that there is a sequence $\{\tilde{A}_i, \tilde{B}_i\}_1^M$ which is a family of rectangular measurable sets closed under bisimulation, which are disjoint and which covers exactly the same data as $\{A_i, B'_i\}_1^N$:

$$\bigcup_{i=1}^{N} A_i \times B'_i = \bigcup_{i=1}^{M} \tilde{A}_i \times \tilde{B}_i.$$

Using this fact we can further expand the equations from (7.1) as follows

$$\begin{aligned} & \mathit{Sup}\left\{\sum_{i=1}^{N}\left(\int_{a\in A_i} f(a)\cdot\int_{b\in B_i}[\![p(a)]\!](b)d\mu_{stochvar(p)}d\mu_D\right)\right\} \\ = \quad & \mathit{Sup}\left\{\sum_{i=1}^{M}\left(\int_{a\in \tilde{A}_i} f(a)\cdot\int_{b\in \tilde{B}_i}[\![p(a)]\!](b)d\mu_{stochvar(p)}d\mu_D\right)\right\}. \end{aligned} \tag{7.3}$$

Note that as the $\tilde{B}_i$ are closed under bisimulation, $Z_i^a \subseteq S/_{\leftrightarrows_{dt}}$ exist such that

$$\int_{b\in\tilde{B}_i}[\![p(a)]\!](b)d\mu_{stochvar(p)} = \mathit{Stoch}(p)(\bigcup Z_i^a).$$

Using this the right hand side of equation (7.3) can be rewritten to

$$\begin{aligned} & \mathit{Sup}\left\{\sum_{i=1}^{M}\left(\int_{a\in\tilde{A}_i} f(a)\cdot \mathit{Stoch}(p)(\bigcup Z_i^a)d\mu_D\right)\right\} \\ \overset{p\leftrightarrows p'}{=} \quad & \mathit{Sup}\left\{\sum_{i=1}^{M}\left(\int_{a\in\tilde{A}_i} f(a)\cdot \mathit{Stoch}(p')(\bigcup Z_i^a)d\mu_D\right)\right\} \\ \overset{\text{Def. 5.6}}{=} \quad & \mathit{Sup}\left\{\sum_{i=1}^{M}\left(\int_{a\in\tilde{A}_i} f(a)\cdot \int_{z\in\mathcal{D}_{p'}(\bigcup Z_i^a)}[\![p']\!](z)d\mu_{stochvar(p')}d\mu_D\right)\right\}. \end{aligned} \tag{7.4}$$

Observe that $\tilde{A}_i \times \tilde{B}_i = \mathcal{D}_{\frac{f}{d:D}p}(\{r(a) \mid a \in \tilde{A}_i, r \in \bigcup Z_i^a\})$ and hence $\{r(a) \mid a \in \tilde{A}_i, r \in \bigcup Z_i^a\} \subseteq \bigcup X$. So, the last equation of (7.4) is equal to

$$\begin{aligned} & \mathit{Sup}\left\{\sum_{i=1}^{M}\int_{\mathcal{D}_{\frac{f}{d:D}p'}(\{r(a)|a\in\tilde{A}_i, r\in\bigcup Z_i^a\})}[\![\frac{f}{d:D}p']\!]d\mu_{D\times stochvar(p')}\right\} \\ = \quad & \mathit{Stoch}(\frac{f}{d:D}p')(\{r(a)|a\in\tilde{A}_i, r\in\bigcup Z_i^a\}) \\ \leq \quad & \mathit{Stoch}(\frac{f}{d:D}p')(\bigcup X). \end{aligned}$$

Note that the argumentation above relies on the fact that $\mathit{Stoch}(\frac{f}{d:D}p')(\bigcup X)$ is defined, ensured as definition 3.8.

$$\mu\left(\mathcal{D}_{\frac{f}{d:D}p'}(\bigcup X)\right) = \mathit{Sup}\left\{\sum_{i=1}^{M}\mu(\tilde{A}_i)\times\mu\left(\mathcal{D}_{\frac{f}{d:D}p'}(Z_i^a)\right)\right\}.$$

In the same way, we can prove the relation

$$\mathit{Stoch}(\frac{f}{d:D}p')(\bigcup X) \leq \mathit{Stoch}(\frac{f}{d:D}p)(\bigcup X)$$

and therefore it must hold that

$$\mathit{Stoch}(\frac{f}{d{:}D}p)(\bigcup X) = \mathit{Stoch}(\frac{f}{d{:}D}p')(\bigcup X).$$

□

Theorem 7.15. Let $\mathcal{A}$ be a measurable data algebra and let $\oplus$ be a process algebra operator such that strong stochastic timed bisimulation equivalence is a congruence for the $\oplus$ operator. Assume the following properties hold:

- $\mathit{stochvar}(p \oplus q) = \mathit{stochvar}(p) \times \mathit{stochvar}(q)$,
- $\llbracket p \oplus q \rrbracket = \lambda \vec{d}{:}\mathit{stochvar}(p), \vec{e}{:}\mathit{stochvar}(q).\ \llbracket p \rrbracket(\vec{d}) \cdot \llbracket q \rrbracket(\vec{e})$, and
- $\mathit{det}(p \oplus q) = \mathit{det}(p) \oplus \mathit{det}(q)$.
- all process expressions are bisimulation resilient wrt. $\mathcal{A}$.

Then, general stochastic bisimulation is also a congruence for the $\oplus$ operator.

Proof. Assume that p, q, p' and q' are general processes such that $p \underline{\leftrightarrow} p'$ and $q \underline{\leftrightarrow} q'$. We must show that $p \oplus q \underline{\leftrightarrow} p' \oplus q'$.

First we concentrate on proving the second property of general stochastic bisimulation, as it is more straightforward than proving the first property. Suppose that (d, e) is possible in $p \oplus q$. Then d is possible in p and e is possible in q. As $p \underline{\leftrightarrow} p'$ and $q \underline{\leftrightarrow} q'$, there is some d' possible in p' such that $\mathit{det}(p)(d) \underline{\leftrightarrow}_{dt} \mathit{det}(p')(d')$ and there is some e' possible in q' such that $\mathit{det}(q)(e) \underline{\leftrightarrow}_{dt} \mathit{det}(q')(e')$. Therefore (d', e') is possible in $p' \oplus q'$ and from the fact that strong stochastic bisimulation is a congruence for $\oplus$, it follows that $\mathit{det}(p)(d) \oplus \mathit{det}(q)(e) \underline{\leftrightarrow}_{dt} \mathit{det}(q)(d') \oplus \mathit{det}(q')(e')$.

For the first part, we must prove that for all $X \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ it is the case that $\mathit{Stoch}(p \oplus q)(\bigcup X) = \mathit{Stoch}(p' \oplus q')(\bigcup X)$. As our processes are bisimulation resilient, $\mathit{Stoch}(p \oplus q)(\bigcup X)$ is defined as follows:

$$\begin{aligned}
\mathit{Stoch}(p \oplus q)(\bigcup X) &\overset{\text{Def. 5.6}}{=} \int_{\mathcal{D}_{p \oplus q}(\bigcup X)} \llbracket p \oplus q \rrbracket \, d\mu_{\mathit{stochvar}(p \oplus q)} \\
&= \int_{(d,e) \in \mathcal{D}_{p \oplus q}(\bigcup X)} \llbracket p \rrbracket(d) \cdot \llbracket q \rrbracket(e) \, d\mu_{\mathit{stochvar}(p) \times \mathit{stochvar}(q)} \qquad (7.5) \\
&\overset{\text{Cor. 3.17}}{=} \mathit{Sup} \left\{ \sum_{i=1}^{N} \left(\int_{a \in A_i} \llbracket p \rrbracket(a) d\mu_{\mathit{stochvar}(p)} \cdot \int_{b \in B_i} \llbracket q \rrbracket(b) d\mu_{\mathit{stochvar}(q)} \right) \right\}
\end{aligned}$$

where the supremum is taken over all possible sequences $\{A_i, B_i\}_1^N$ such that A_i, B_i are measurable, $\bigcup_{i=1}^N A_i \times B_i \subseteq \mathcal{D}_{p \oplus q}(\bigcup X)$ and $A_i \times B_i$ are mutually disjoint.

So, the integral has been approximated with an arbitrary precision by a sum of integrals over some disjoint finite collection of measurable rectangular sets. But we require a stronger property namely that this integral can be approximated using sequences $\{(A_i, B_i)\}_1^N$ such that both A_i and B_i are closed under bisimulation, i.e., for all $d \in A_i$ and $d' \in \mathit{stochvar}(p) \backslash A_i$ it holds $\mathit{det}(p)(d) \not\underline{\leftrightarrow}_{dt} \mathit{det}(p)(d')$ and for all $e \in B_i$ and $e' \in \mathit{stochvar}(p) \backslash B_i$ it holds $\mathit{det}(q)(e) \not\underline{\leftrightarrow}_{dt} \mathit{det}(q)(e')$.

First we show that for every family of disjoint measurable rectangular sets $\{(A_i, B_i)\}_1^N$ such that $\bigcup_{i=1}^N A_i \times B_i \subseteq \mathcal{D}_{p \oplus q}(\bigcup X)$ there is a family of not necessarily disjoint rectangular sets $\{(A_i', B_i')\}_1^N$ such that A_i' and B_i' are closed under bisimulation and

$$\bigcup_{i=1}^{N} A_i \times B_i \subseteq \bigcup_{i=1}^{N} A_i' \times B_i' \subseteq \mathcal{D}_{p \oplus q}(\bigcup X) \qquad (7.6)$$

The sets A_i' and B_i' are constructed as the closure under bisimulation of A_i, resp. B_i as follows

$$A_i' = \mathcal{D}_p(\{r \mid \exists d \in A_i . r \underline{\leftrightarrow}_{dt} \mathit{det}(p)(d)\}),$$

$$B'_i = \mathcal{D}_q(\{r | \exists e \in B_i . r \underline{\leftrightarrow}_{dt}\ det(q)(e)\}).$$

As $A_i \subseteq A'_i$ and $B_i \subseteq B'_i$, the set inclusion at the left of equation (7.6) holds trivially. We have yet to prove the set inclusion at the right. Suppose for some a' and b' that $(a', b') \in A'_i \times B'_i$. Then there must be some $(a, b) \in A_i \times B_i$ such that $det(p)(a) \underline{\leftrightarrow}_{dt} det(p)(a')$ and $det(q)(b) \underline{\leftrightarrow}_{dt} det(q)(b')$. From the congruence of strong stochastic bisimulation for $\oplus$ it follows that $det(q)(a) \oplus det(q)(b) \underline{\leftrightarrow}_{dt}\ det(p)(a') \oplus det(q)(b')$. Hence, as $\mathcal{D}_{p \oplus q}(\bigcup X)$ is closed under bisimulation and $(a, b) \in \mathcal{D}_{p \oplus q}(\bigcup X)$, we find $(a', b') \in \mathcal{D}_{p \oplus q}(\bigcup X)$. Therefore every $A'_i \times B'_i$ is a subset of $\mathcal{D}_{p \oplus q}(\bigcup X)$ and thus the union $\bigcup_{i=1}^{N} A'_i \times B'_i$ has to be a subset of $\mathcal{D}_{p \oplus q}(\bigcup X)$, too.

Observe that lemma 6.3 implies that all A'_i and B'_i are measurable. Given the sequence $\{A'_i, B'_i\}_1^N$ it follows using lemma 7.13 that there exists a sequence $\{\tilde{A}_i, \tilde{B}_i\}_1^M$ which is a family of disjoint rectangular measurable sets closed under bisimulation that covers exactly the same data as $\{A'_i, B'_i\}_1^N$, i.e.,

$$\bigcup_{i=1}^{N} A'_i \times B'_i = \bigcup_{i=1}^{M} \tilde{A}_i \times \tilde{B}_i .$$

Combining, these we can replace the last lines of the equalities (7.5) by

$$\begin{aligned}\int_{(d,e) \in \mathcal{D}_{p \oplus q}(\bigcup X)} \llbracket p \rrbracket(d) \cdot \llbracket q \rrbracket(e)\, d\mu_{stochvar(p) \times stochvar(q)} \quad &= \\ Sup \left\{ \sum_{i=1}^{M} \left(\int_{a \in \tilde{A}_i} \llbracket p \rrbracket(a) d\mu_{stochvar(p)} \cdot \int_{b \in \tilde{B}_i} \llbracket q \rrbracket(b) d\mu_{stochvar(q)} \right) \right\}&\end{aligned} \tag{7.7}$$

where the supremum is taken over all possible sequences $\{\tilde{A}_i, \tilde{B}_i\}_1^M$ such that $\tilde{A}_i$ and $\tilde{B}_i$ are measurable, mutually disjoint, closed under bisimulation and $\bigcup_{i=1}^{M} \tilde{A}_i \times \tilde{B}_i \subseteq \mathcal{D}_{p \oplus q}(\bigcup X)$.

Note that as $\tilde{A}_i$ and $\tilde{B}_i$ are closed under bisimulation, there must be some $Y_i, Z_i \subseteq S/_{\underline{\leftrightarrow}_{dt}}$ such that

$$\int_{a \in \tilde{A}_i} \llbracket p \rrbracket(a) d\mu_{stochvar(p)} = Stoch(p)(\bigcup Y_i) \quad \text{and} \quad \int_{b \in \tilde{B}_i} \llbracket q \rrbracket(b) d\mu_{stochvar(q)} = Stoch(q)(\bigcup Z_i).$$

Continuing with equation (7.7), we obtain

$$\begin{aligned} & Sup \left\{ \sum_{i=1}^{M} \left(\int_{a \in \tilde{A}_i} \llbracket p \rrbracket(a) d\mu_{stochvar(p)} \cdot \int_{b \in \tilde{B}_i} \llbracket q \rrbracket(b) d\mu_{stochvar(q)} \right) \right\} \\ = \quad & Sup \left\{ \sum_{i=1}^{M} \left(Stoch(p)(\bigcup Y_i) \cdot Stoch(q)(\bigcup Z_i) \right) \right\} \\ \overset{p \underline{\leftrightarrow} p'\ q \underline{\leftrightarrow} q'}{=} \quad & Sup \left\{ \sum_{i=1}^{M} \left(Stoch(p')(\bigcup Y_i) \cdot Stoch(q')(\bigcup Z_i) \right) \right\} \\ \overset{\text{Def. 5.6}}{=} \quad & Sup \left\{ \sum_{i=1}^{M} \left(\int_{y \in \mathcal{D}_{p'}(\bigcup Y_i)} \llbracket p' \rrbracket(y) d\mu_{stochvar(p')} \cdot \int_{z \in \mathcal{D}_{q'}(\bigcup Z_i)} \llbracket q' \rrbracket(z) d\mu_{stochvar(q')} \right) \right\} \\ \overset{\text{Th. 3.14}}{=} \quad & Sup \left\{ \sum_{i=1}^{M} \int_{\mathcal{D}_{p' \oplus q'}(\{r \oplus r' | r \in \bigcup Y_i, r' \in \bigcup Z_i\})} \llbracket p' \oplus q' \rrbracket d\mu_{stochvar(p' \oplus q')} \right\} \\ \overset{\text{Def. 5.6}}{=} \quad & Sup \left\{ \sum_{i=1}^{M} Stoch(p' \oplus q')(\{r \oplus r' | r \in \bigcup Y_i, r' \in \bigcup Z_i\}) \right\} . \end{aligned}$$

Note that $\tilde{A}_i \times \tilde{B}_i = \mathcal{D}_{p\oplus q}(\{r \oplus r' | r \in \bigcup Y_i, r' \in \bigcup Z_i\})$ and hence $\bigcup_{i=1}^{M} \{r \oplus r' | r \in \bigcup Y_i, r' \in \bigcup Z_i\} \subseteq \bigcup X$. So we can conclude

$$Sup \left\{ \sum_{i=1}^{M} Stoch(p' \oplus q')(\{r \oplus r' | r \in \bigcup Y_i, r' \in \bigcup Z_i\}) \right\} \leq Stoch(p' \oplus q')(\bigcup X).$$

Analogically, we can prove the relation

$$Stoch(p' \oplus q')(\bigcup X) \leq Stoch(p \oplus q)(\bigcup X)$$

and therefore it must hold that

$$Stoch(p \oplus q)(\bigcup X) = Stoch(p' \oplus q')(\bigcup X).$$

□

Corollary 7.16. Let $\mathcal{A}$ be a measurable data algebra and assume all process expressions are bisimulation resilient wrt. $\mathcal{A}$. Then general stochastic bisimulation is a congruence for the $+$, $\|$ and $b{\rightarrow}\_\diamond\_$ operators.

8 Conclusion and future research

In this document we gave a natural semantics for a process language with a stochastic operator. We provided a notion of bisimulation resilience that guarantees that stochastic processes in a setting with bisimulation make sense. Furthermore, we introduced notions of bisimulation for determined and general stochastic processes. With examples we motivated the choices we made in the definitions. With quite elaborate proofs it was shown that these bisimulations are congruences.

An interesting issue is the translation of the semantic notion of bisimulation resilience to the syntax of processes. Which data expressions can safely be used in processes, such that its stochastic behaviour is well defined? We have not addressed this issue, yet, but it one of the first on our list because it is essential to know in order to use the language.

We omitted the general sum operator in our language as it adds a next layer of complexity. Recall that the generalised sum operator

$$\sum_{d:D} p$$

offers a choice in behaviour for any d from D. If D is finite the sum operator can be dealt with in the framework of this paper by expanding it to the choice operator. But the sum operator is particularly useful and interesting when D is infinite (e.g., $D{=}\mathbb{N}$), or even uncountably infinite (e.g., $D{=}\mathbb{R}$, $D{=}\mathbb{R} \rightarrow \mathbb{R}$, etc.). In order to define the semantics of the sum operator, we must extend definition 5.4 with some clause of the form

$$[\![\sum_{d:D} p]\!] = \lambda\vec{e}{:}stochvar(p).\prod_{d:D} [\![p]\!](\vec{e}).$$

But in this formulation, the (uncountably) infinite product does not have a proper definition as $[\![p]\!](\vec{e})$ can have arbitrary values. If in a product $\prod_{i\in I} r_i$ it holds that $0{\leq}r_i{\leq}1$, the product can be properly defined. We expect that this can be employed by reformulating the semantics in this paper in terms of probabilities, instead of distribution functions, but we decided to defer this to a next paper given the technical complexity of the current paper.

Besides the semantics of sum operator, much more needs to be done to bring this process algebra in par with the theories for standard process algebras with data but without stochastic operators. This requires definitions of variants of weak bisimulation, an algebraic characterisation of the equivalences, definition of recursive processes (what happens when the stochastic operator occurs unguarded in recursive processes?), manual proof methodology and the construction of tools and algorithms. We intend to conquer all these issues one at a time.

References

[1] S. Andova. *Probabilistic Process Algebra*. PhD thesis, Technische Universiteit Eindhoven, 2002.

[2] S. Banach and A. Tarski. Sur la décomposition des ensembles de points en parties respectivement congruentes. *Fundamenta Mathematicae*, 6:244-277, 1924.

[3] M. Bravetti and P.R. D'Argenio. Tutte le algebre insieme: Concepts, discussions and relations of stochastic process algebras with general distributions. In *Validation of Stochastic Systems*, pages 44–88, 2004.

[4] L. Cardelli and R. Mardare. The measurable space of stochastic processes. In *QEST*, pages 171–180, 2010.

[5] S. Cattani, R. Segala, M.Z. Kwiatkowska, and G. Norman. Stochastic transition systems for continuous state spaces and non-determinism. In *FoSSaCS*, pages 125–139, 2005.

[6] V. Danos, J. Desharnais, F. Laviolette and Prakash Panangaden. Bisimulation and cocongruence for probabilistic systems. Information and Computation 204(4), 503-523, 2006.

[7] P.R. D'Argenio. *Algebras and Automata for Timed and Stochastic Systems*. PhD thesis, University of Twente, 1999.

[8] P.R. D'Argenio and J.-P. Katoen. A theory of stochastic systems. Part II: Process Algebra. Information and Computation 203:39-74, 2005.

[9] J.F. Groote, A.H.J. Mathijssen, M.A. Reniers, Y.S. Usenko, and M.J. van Weerdenburg. Analysis of distributed systems with mCRL2. In M. Alexander, W. Gardner, editors, Process Algebra for Parallel and Distributed Processing. Chapman Hall, pp. 99-128, 2009.

[10] J.F. Groote and M.A. Reniers. Algebraic process verification. In J.A. Bergstra, A. Ponse and S.A. Smolka. Handbook of Process Algebra, pages 1151-1208, Elsevier, Amsterdam, 2001.

[11] D. Van Hung and M. Wirsing, editors. *Theoretical Aspects of Computing - ICTAC 2005, Second International Colloquium, Hanoi, Vietnam, October 17-21, 2005, Proceedings*, volume 3722 of *Lecture Notes in Computer Science*. Springer, 2005.

[12] J.P. Katoen, J.C. van de Pol, M.I.A. Stoelinga and M. Timmer. A linear process-algebraic format for probabilistic systems with data. In: Application of Concurrency to System Design, Tenth International Conference, Braga, Portugal. pp. 213-222. IEEE Computer Society Press. 2010.

[13] A. Hinton, M. Kwiatkowska, G. Norman and D. Parker. PRISM: A tool for automatic verification of probabilistic systems. In H. Hermanns and J. Palsberg (editors) Proc. 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'06), volume 3920 of Lecture Notes in Computer Science, pages 441-444, Springer-Verlag, 2006.

[14] K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. Information and Computation. 94(1):1-28, 1991.

[15] B. Klin and V. Sassone. Structural operational semantics for stochastic process calculi. In *FoSSaCS*, pages 428–442, 2008.

[16] R. Lanotte and S. Tini. Probabilistic congruence for semistochastic generative processes. In *FoSSaCS*, pages 63–78, 2005.

[17] M.E. Taylor. *Measure Theory and Integration*. The American Mathematical Society, 2006.

[18] E.P. de Vink and J.J.M.M. Rutten. Bisimulation for probabilistic transition systems: A coalgebraic approach. *Theor. Comput. Sci.*, 221(1-2):271–293, 1999.