UNIVERSITY OF OSLO
Department of Informatics

A denotational model for component-based risk analysis

Research report 363

Gyrd Brændeland

Atle Refsdal

Ketil Stølen

ISBN 82-7368-321-4
ISSN 0806-3036

February 2011

A denotational model for component-based risk analysis

Gyrd Brændeland[a,b], Atle Refsdal[a], Ketil Stølen[a,b]

[a]*SINTEF ICT, Oslo, Norway*
[b]*Department of Informatics, University of Oslo, Norway*

Abstract

Risk analysis is an important tool for developers to establish the appropriate protection level of a system. Unfortunately, the shifting environment of components and component-based systems is not adequately addressed by traditional risk analysis methods. This report addresses this problem from a theoretical perspective by proposing a denotational model for component-based risk analysis. In order to model the probabilistic aspect of risk, we represent the behaviour of a component by a probability distribution over communication histories. The overall goal is to provide a theoretical foundation facilitating an improved understanding of risk in relation to components and component-based system development.

Key words: Risk analysis, component-based development, denotational semantics

Contents

1. Introduction

The flexibility offered by component-based development techniques, such as Sun's Enterprise JavaBeans (EJB) [39] and Microsoft's .NET [36], and the potential for reducing production costs through reuse, has lead to an increased preference for such techniques. With strict time-to-market requirements for software technology, products such as cars, laptops, smart phones and mobile devices in general are increasingly sold with upgradeable parts. The flexibility offered by component-based development facilitates rapid development and deployment, but causes challenges for risk analysis that are not addressed by current methods.

An important question for users and developers of component technology is whether to trust a new component to be integrated into a system. This is especially true for systems that handle safety and security-critical tasks such as flight-control systems, or accounting systems [30, 11]. Output from traditional risk-analysis methods is, however, difficult to apply to modern software design. Furthermore, few traditional risk analysis methods take into account that the risk level towards component-based systems may change, given changes in the environment of the systems [53, 33].

There are many forms and variations of risk analysis, depending on the application domain, such as finance, reliability and safety, or security. In finance risk analysis is concerned with balancing potential gain against risk of investment loss. In this setting a risk can be both positive and negative. Within reliability and safety or security, which are the most relevant for component-based development, risk analysis is concerned with protecting existing assets from harm. We focus upon the latter type of risk analysis, referred to in the following as asset-driven risk analysis. In asset-driven risk analysis, the analysis of threats, vulnerabilities and incidents are driven by the identified assets. An asset may be anything of value to the client of the risk analysis, such as information, software, hardware, services or human life. Assets may also be purely conceptual, such as for example the reputation of an organisation.

The purpose of asset-driven risk analysis is to gather sufficient knowledge about vulnerabilities, threats, consequences and probabilities, in order to establish the appropriate protection level for assets. It is important that the level of protection matches the value of the assets to be protected. If the protection level is too low, the cost from risks will be too high. If the protection level is too high, it may render a service inconvenient for users. A certain level of risk may be acceptable if the risk is considered to be too costly or technically impossible to rule out entirely. Hence, a risk is part of the behaviour of a system that is implicitly allowed but not necessarily intended. Based on this observation we define a component model that integrates the explicit representation of risks as part of the component behaviour and provides rules for composing component risks. We also explain how the notion of hiding can be understood in this component model. We define a hiding operator that allows partial hiding of internal interactions, to ensure that interactions affecting the component risk level are not hidden. We are not aware of other approaches where the concept of risk is integrated in a formal component semantics.

An advantage of representing risks as part of the component behaviour, is that the risk level of a composite component, as well as its behaviour, is obtained by composing the representations of its sub-components. That is, the composition of risks corresponds to ordinary component composition. The component model provides a foundation for component-based risk analysis, by conveying how risks manifests themselves in an underlying component implementation. By component-based risk analysis we mean that risks are identified, analysed and documented at the component level, and that risk analysis results are composable. The objective of component-based risk analysis is to support development of components that are both trustworthy and user friendly by aiding developers in selecting appropriate protection levels for component assets and develop components in accordance with the selected protection level.

Understanding risks in a component-based setting is challenging because the concept of risk traditionally incorporates some knowledge about how the environment behaves. In order to define a formal foundation for component-based risk analysis, we must decide which risk concepts to include at the component level, without compromising the modularity of our components. In conventional risk analysis external threats are often included and their likelihoods are analysed as part of the overall analysis. The rationale is that the likelihood of an incident is determined from various factors, including the motivation and resources of a potential threat. In a component-based setting, however, we cannot expect to have knowledge about the environment of the component as that may change depending on the platform it is deployed in. Moreover, it is a widely adopted requirement to components that they are separated from their environment and other components, in order to be independently deployable. This distinction is provided by a clear specification of the component interfaces and by encapsulating the component implementation [6]. In order to obtain a method for component-based risk analysis, current methods must be adapted to comply with the same principles of modularity and composition as component-based development.

1.1. Outline of report

The objective of Section 2 is to give an informal understanding of component-based risk analysis. Risk is the probability that an event affects an asset with a given consequence. In order to model component risks, we explain the concept of asset, asset value and consequence in a component setting. In order to represent the *behavioural* aspects of risk, such as the probability of unwanted incidents, we make use of an asynchronous communication paradigm. The selection of this paradigm is motivated as part of the informal explanation of component-based risk analysis. We also explain the notions of observable and unobservable behaviour in a component model with assets. The informal understanding introduced in Section 2 is thereafter formalised in a semantic model that defines:

– The denotational representation of interfaces as probabilistic processes (Section 3).

– The denotational representation of interface risks including the means to represent risk probabilities (Section 4). Interface risks are incorporated as a part of the interface behaviour.

– The denotational representation of a component as a collection of interfaces or sub-components, some of which may interact with each other (Section 5). We obtain the behaviour of a component from the probabilistic processes of its constituent interfaces or sub-components in a basic mathematical way.

– The denotational representation of component risks (Section 6).

– The denotational representation of hiding (Section 7).

We place our work in relation to ongoing research within related areas in Section 8. Finally we summarise our findings and discuss possibilities for future work in Section 9.

2. An informal explanation of component-based risk analysis

In this section we describe informally the notion of component-based risk analysis that we aim to formalise in the later sections of this report. In Section 2.1 we explain the concepts of risk analysis and how they relate in a conceptual model. In Section 2.2 we explain the conceptual component model, and in Section 2.3 we explain how the two conceptual models relate to each other. In Section 2.4 we motivate the selection of communication paradigm and explain the behaviour of probabilistic component interfaces. In Section 2.5 we explain which behaviour should be observable in a component with assets, and which should be hidden.

2.1. Risk analysis

Risk analysis is the systematic process to understand the nature of and to deduce the level of risk [48]. We explain the concepts of risk analysis and how they are related to each other through the conceptual model, captured by a UML class diagram [40] in Figure 1. The risk concepts are adapted from international standards for risk analysis terminology [48, 18, 17]. The associations between the elements have cardinalities specifying the number of instances of one element that can be related to one instance of the other. The hollow diamond symbolises aggregation and the filled composition. Elements connected with an aggregation can also be part of other aggregations, while composite elements only exist within the specified composition.

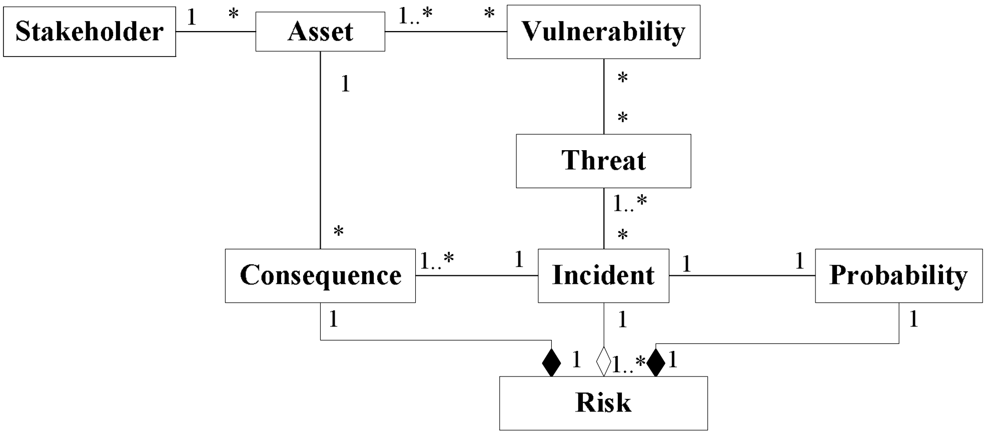

Figure 1: Conceptual model of risk analysis

We explain the conceptual model as follows: *Stakeholders* are those people and organisations who are affected by a decision or activity. An *asset* is something to which a stakeholder directly assigns value and, hence, for which the stakeholder requires protection. An asset is uniquely linked to its stakeholder. An *event* refers to the occurrence of a particular circumstance. An event which reduces the value of at least one asset is referred to as an *incident*. A *consequence* is the reduction in value caused by an incident to an asset. It can be measured qualitatively by linguistic expressions such as "minor", "moderate", "major", or quantitatively, such as a monetary value. A *vulnerability* is a weakness which can be exploited by one or more threats. A *threat* is a potential cause of an incident. It may be external (e.g., hackers or viruses) or internal (e.g., system failures). Furthermore, a threat may be intentional, i.e., an attacker, or unintentional, i.e., someone causing an incident by mistake. *Probability* is a measure of the chance of occurrence of an event, expressed as a number between 0 and 1. Conceptually, as illustrated by the UML class diagram in Figure 1, a *risk* consists of an incident, its probability, and its consequence with regard to a given asset. There may be a range of possible outcomes associated with an incident. This implies that an incident may have consequences for several assets. Hence, an incident may be part of several risks.

2.2. Components and interfaces

Intuitively a component is a standardised "artefact" that can be mass-fabricated and reused in various constellations. According to the classical definition by Szyperski, a software component

> ... is a unit of composition with contractually specified interfaces and explicit context dependencies only. A software component can be deployed independently and is subject to composition by third parties [49].

That a component is a unit of independent deployment means that it needs to be well separated from its environment and other components. A component, therefore, encapsulates its constituent parts. A third party is one that cannot be expected to have access to the construction details of the components involved. A component therefore needs to be sufficiently self-contained.

Components interact through interfaces. An interface is often seen as a contract, specifying what it will provide given that the environment fulfils certain conditions or assumptions. Cheesman and Daniels [4] distinguish between usage and realisation contracts. According to their component definition a component is a realisation contract describing provided interfaces and component dependencies in terms of required interfaces. A provided interface is a usage contract, describing a set of operations provided by a component object.

Our component model is illustrated in Figure 2. To keep the component model simple and general we do not distinguish between usage and realisation. A *component* is simply a collection of interfaces some of which may interact with each other. Interfaces interact by the transmission and consumption of messages. We refer to the transmission and consumption of messages as *events*.

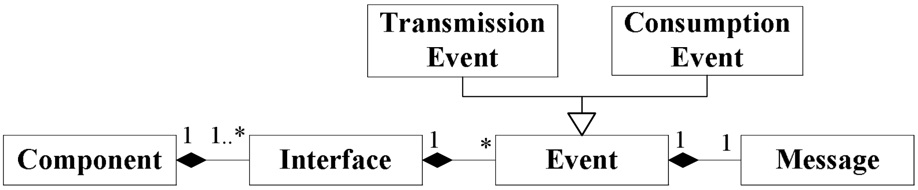

Figure 2: Conceptual component model

2.3. Component-based risk analysis

Figure 3 shows how the conceptual model of risk analysis relates to the conceptual component model. To ensure modularity of our component model we represent a stakeholder by the component interface, and identify assets on behalf of component interfaces. Each interface has a set of assets. Hence, the concept of a stakeholder is implicitly present in the integrated conceptual model, through the concept of an interface[1]. A vulnerability may be understood as a property (or lack thereof) of an interface that makes it prone to a certain attack. It may therefore be argued that the vulnerability concept should be associated to the interface concept. However, from a risk perspective a vulnerability is relevant to the extent that it can be exploited to harm a specific asset, and we have therefore chosen to associate it with the asset concept. The concept of a threat is not part of the conceptual model, because a threat is something that belongs to the environment of a component. We cannot expect to have knowledge about the environment of the component as that may change depending on the where it is deployed. An event that harms an asset is an incident with regard to that asset. An event is as explained above either the consumption or the transmission of a message by an interface. Moreover, a consequence is a measure on the level of seriousness of an incident with regard to an asset.

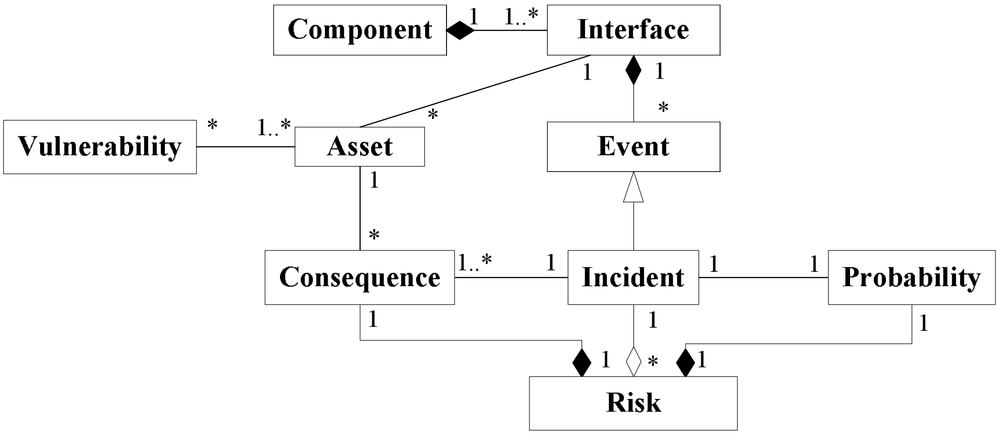

Figure 3: Conceptual model of component-based risk analysis

2.4. Behaviour and probability

A probabilistic understanding of component behaviour is required in order to measure risk. We adopt an asynchronous communication model. This does not prevent us from representing systems with synchronous communication. It is well known that synchronous communication can be simulated in an asynchronous communication model and the other way around [16].

[1] Note that there may be interfaces with no assets; in this case the stakeholder corresponding to the interface has nothing to protect.

An interface interacts with an environment whose behaviour it cannot control. From the point of view of the interface the choices made by the environment are non-deterministic. In order to resolve the external non-determinism caused by the environment we use queues that serve as schedulers. Incoming messages to an interface are stored in a queue and are consumed by the interface in the order they are received. The idea is that, for a given sequence of incoming messages to an interface, we know the probability with which the interface produces a certain behaviour. For simplicity we assume that an interface does not send messages to itself.

A component is a collection of interfaces some of which may interact. For a component consisting of two or more interfaces, a queue history not only resolves the external non-determinism, but also all internal non-determinism with regard to the interactions of its sub-components. The behaviour of a component is the set of probability distributions given all possible queue histories of the component.

Figure 4 shows two different ways in which two interfaces n_1 and n_2 with queues q_1 and q_2, and sets of assets a_1 and a_2, can be combined into a component. We may think of the arrows as directed channels.

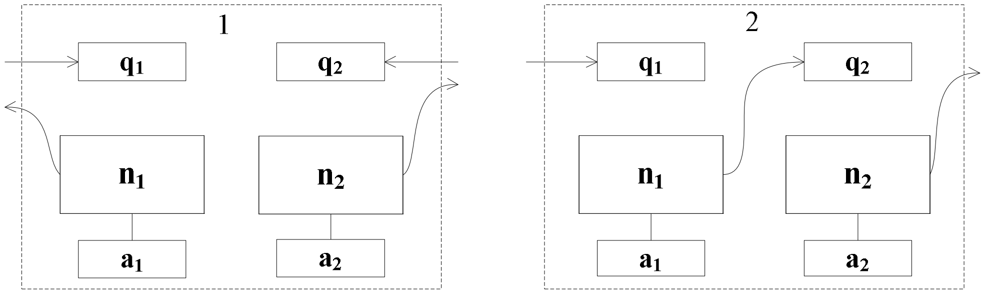

Figure 4: Two interface compositions

- In Figure 4 (1) there is no direct communication between the interfaces of the component, that is, the queue of each interface only contains messages from external interfaces.

- In Figure 4 (2) the interface n_1 transmits to n_2 which again transmits to the environment. Moreover, only n_1 consumes messages from the environment.

Initially, the queue of each interface is empty; its set of assets is fixed throughout an execution. When initiated, an interface chooses probabilistically between a number of different actions (as described in Figure 5). An action consists of transmitting an arbitrary number of messages in some order. The number of transmission messages may be finite, including zero which corresponds to the behaviour of skip, or infinite. The storing of a transmitted message in a queue is instantaneous: a transmitted message is placed in the queue of the recipient, without time delay. There will always be some delay between the transmission of a message and the consumption of that message. After transmitting messages the interface may choose to quit or to check its queue for messages. Messages are consumed in the order they arrive. If the queue is empty, an attempt to consume

```
while true do
begin
    probabilistic_choice(action$_1$, ..., action$_m$);
    if done then break;
    blocking_consume(message);
end
```

Figure 5: Pseudo-code for the input-output behaviour of an interface

blocks the interface from any further action until a new message arrives. The consumption of a message gives rise to a new probabilistic choice. Thereafter, the interface may choose to quit without checking the queue again, and so on.

A probabilistic choice over actions never involves more than one interface. This can always be ensured by decomposing probabilistic choices until they have the granularity required. Suppose we have three interfaces; die, player1 and player2 involved in a game of Monopoly. The state of the game is decided by the position of the players' pieces on the board. The transition from one state to another is decided by a probabilistic choice "Throw die and move piece", involving both the die and one of the players. We may however, split this choice into two separate choices: "Throw die" and "Move piece". By applying this simple strategy for all probabilistic choices we ensure that a probabilistic choice is a local event of an interface.

The probability distribution over a set of actions, resulting from a probabilistic choice, may change over time during an execution. Hence, our probabilistic model is more general than for example a Markov process [54, 34], where the probability of a future state given the present is conditionally independent of the past. This level of generality is needed to be able to capture all types of probabilistic behaviour relevant in a risk analysis setting, including human behaviour.

The behaviour of a component is completely determined by the behaviour of its constituent interfaces. We obtain the behaviour of a component by starting all the interfaces simultaneously, in their initial state.

2.5. Observable component behaviour

In most component-based approaches there is a clear separation between external and purely internal interaction. External interaction is the interaction between the component and its environment; while purely internal interaction is the interaction within the components, in our case, the interaction between the interfaces of which the component consists. Contrary to the external, purely internal interaction is hidden when the component is viewed as a black-box.

When we bring in the notion of risk, this distinction between what should be externally and only internally visible is no longer clear cut. After all, if we blindly hide all internal interaction we are in danger of hiding (without treating) risks of relevance for assets belonging to externally observable interfaces. Hence, purely internal interaction should be externally visible if it may affect assets belonging to externally visible interfaces. Consider for example the component pictured in Figure 6. In a conventional component-oriented approach, the channels i_2, i_3, o_2 and o_3 would not be externally observable from a black-box point of view. From a risk analysis perspective it seems more

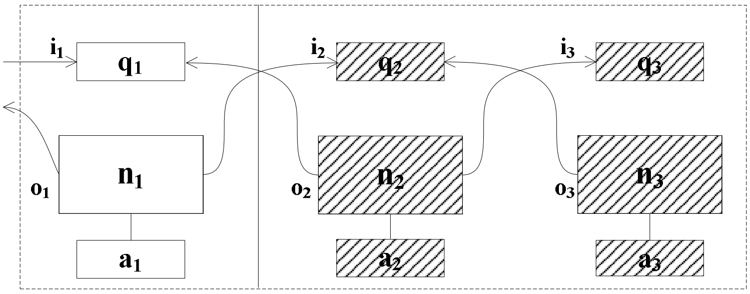

Figure 6: Hiding of unobservable behaviour

natural to restrict the black-box perspective to the right hand side of the vertical line. The assets belonging to the interface n_1 are externally observable since the environment interacts with n_1. The assets belonging to the interfaces n_2 and n_3 are on the other hand hidden since n_2 and n_3 are purely internal interfaces. Hence, the channels i_3 and o_3 are also hidden since they can only impact the assets belonging to n_1 indirectly via i_2 and o_2. The channels i_2 and o_2 are however only partly hidden since the transmission events of i_2 and the consumption events of o_2 may include incidents having an impact on the assets belonging to n_1.

3. Denotational representation of interface behaviour

In this section we explain the formal representation of interface behaviour in our denotational semantics. We represent interface behaviour by sequences of events that fulfil certain well-formedness constraints. Sequences fulfilling these constraints are called traces. We represent probabilistic interface behaviour as probability distributions over sets of traces.

3.1. Sets

We use standard set notation, such as *union* $A \cup B$, *intersection* $A \cap B$, set difference $A \setminus B$, *cardinality* $\#A$ and *element of* $e \in A$ in the definitions of our basic concepts and operators. We write $\{e_1, e_2, e_3, \ldots, e_n\}$ to denote the set consisting of n elements $e_1, e_2, e_3, \ldots, e_n$. Sometimes we also use $[i..n]$ to denote a totally ordered set of numbers between i and n. We introduce the special symbol $\mathbb{N}$ to denote the set of *natural numbers*:

$$\mathbb{N} \overset{\mathsf{def}}{=} \{0, 1, 2, 3, \ldots, n, n+1, \ldots\}$$

and $\mathbb{N}_+$ to denote the set of strictly positive natural numbers:

$$\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$$

3.2. Events

There are two kinds of events: transmission events tagged by ! and consumption events tagged by ?. $\mathcal{K}$ denotes the set of kinds $\{!, ?\}$. An event is a pair of a kind and a message. A message is a quadruple $\langle s, tr, co, q \rangle$ consisting of a signal s, a transmitter

tr, a consumer co and a time-stamp q, which is a rational number. The consumer in the message of a transmission event coincides with the addressee, that is, the party intended to eventually consume the message.

The *active* party in an event is the one performing the action denoted by its kind. That is, the transmitter of the message is the active party of a transmission event and the consumer of the message is the active party of a consumption event.

We let $\mathcal{S}$ denote the set of all signals, $\mathcal{P}$ denote the set of all parties (consumers and transmitters), $\mathcal{Q}$ denote the set of all time-stamps, $\mathcal{M}$ denote the set of all messages and $\mathcal{E}$ denote the set of all events. Formally we have that:

$$\begin{aligned}\mathcal{E} &\stackrel{\mathsf{def}}{=} \mathcal{K} \times \mathcal{M}\\ \mathcal{M} &\stackrel{\mathsf{def}}{=} \mathcal{S} \times \mathcal{P} \times \mathcal{P} \times \mathcal{Q}\end{aligned}$$

We define the functions

$$k.\_ \in \mathcal{E} \rightarrow \mathcal{K} \quad tr.\_, co.\_ \in \mathcal{E} \rightarrow \mathcal{P} \quad q.\_ \in \mathcal{E} \rightarrow \mathcal{Q}$$

to yield the kind, transmitter, consumer and time-stamp of an event. For any party $p \in \mathcal{P}$, we use $\mathcal{E}_p$ to denote the set of all events in which p is the active part. Formally

$$(1) \qquad \mathcal{E}_p \stackrel{\mathsf{def}}{=} \{e \in \mathcal{E} \mid (k.e = ! \wedge tr.e = p) \vee (k.e = ? \wedge co.e = p)\}$$

For a given party p, we assume that the number of signals assigned to p is a most countable. That is, the number of signals occurring in messages consumed by or transmitted to p is at most countable.

We use $\mathcal{E}_p^{\downarrow}$ to denote the set of transmission events with p as consumer. Formally

$$\mathcal{E}_p^{\downarrow} \stackrel{\mathsf{def}}{=} \{e \in \mathcal{E} \mid k.e = ! \wedge co.e = p\}$$

3.3. Sequences

For any set of elements A, we let A^{ω}, A^{∞}, A^{*} and A^{n} denote the set of all sequences, the set of all infinite sequences, the set of all finite sequences, and the set of all sequences of length n over A. We use $\langle\rangle$ to denote the empty sequence of length zero and $\langle 1, 2, 3, 4\rangle$ to denote the sequence of the numbers from 1 to 4. A sequence over a set of elements A can be viewed as a function mapping positive natural numbers to elements in the set A. We define the functions

$$(2) \qquad \#\_ \in A^{\omega} \rightarrow \mathbb{N} \cup \{\infty\} \quad \_ \sqsubseteq \_ \in A^{\omega} \times A^{\omega} \rightarrow \mathbb{B}\mathrm{ool}$$

to yield the length, the nth element of a sequence and the prefix ordering on sequences[2]. Hence, $\#s$ yields the number of elements in s, $s[n]$ yields s's nth element if $n \leq \#s$, and $s_1 \sqsubseteq s_2$ evaluates to true if s_1 is an initial segment of s_2 or if $s_1 = s_2$.

[2] The operator × binds stronger than → and we therefore omit the parentheses around the argument types in the signature definitions.

For any $0 \leq i \leq \#s$ we define $s|_i$ to denote the prefix of s of length i. Formally:

(3)
$$\_|\_ \in A^{\omega} \times \mathbb{N} \rightarrow A^{\omega}$$
$$s|_i \overset{\mathsf{def}}{=} \begin{cases} s' \text{ if } 0 \leq i \leq \#s, \text{ where } \#s' = i \wedge s' \sqsubseteq s \\ s \text{ if } i > \#s \end{cases}$$

Due to the functional interpretation of sequences, we may talk about the *range* of a sequence:

(4)
$$\mathsf{rng}.\_ \in A^{\omega} \rightarrow \mathbb{P}(A)$$

For example if $s \in A^{\infty}$, we have that:

$$\mathsf{rng}.s = \{s[n] \mid n \in \mathbb{N}_+\}$$

We define an operator for obtaining the sets of events of a set of sequences, in terms of their ranges:

(5)
$$ev.\_ \in \mathbb{P}(A^{\omega}) \rightarrow \mathbb{P}(A)$$
$$ev.S \overset{\mathsf{def}}{=} \bigcup_{s \in S} \mathsf{rng}.s$$

We also define an operator for concatenating two sequences:

(6)
$$\_ \frown \_ \in A^{\omega} \times A^{\omega} \rightarrow A^{\omega}$$
$$s_1 \frown s_2[n] \overset{\mathsf{def}}{=} \begin{cases} s_1[n] \text{ if } 1 \leq n \leq \#s_1 \\ s_2[n - \#s_1] \text{ if } \#s_1 < n \leq \#s_1 + \#s_2 \end{cases}$$

Concatenating two sequences implies gluing them together. Hence $s_1 \frown s_2$ denotes a sequence of length $\#s_1 + \#s_2$ that equals s_1 if s_1 is infinite and is prefixed by s_1 and suffixed by s_2, otherwise.

The filtering function Ⓢ is used to filter away elements. By B Ⓢ s we denote the sequence obtained from the sequence s by removing all elements in s that are not in the set of elements B. For example, we have that

$$\{1,3\} \circledS \langle 1,1,2,1,3,2 \rangle = \langle 1,1,1,3 \rangle$$

We define the filtering operator formally as follows:

(7)
$$\_ \circledS \_ \in \mathbb{P}(A) \times A^{\omega} \rightarrow A^{\omega}$$
$$B \circledS \langle\rangle \overset{\mathsf{def}}{=} \langle\rangle$$
$$B \circledS (\langle e \rangle \frown s) \overset{\mathsf{def}}{=} \begin{cases} \langle e \rangle \frown B \circledS s & \text{if } e \in B \\ B \circledS s & \text{if } e \notin B \end{cases}$$

For an infinite sequence s we need the additional constraint:

$$(B \cap \mathsf{rng}.s) = \emptyset \Rightarrow B \circledS s = \langle\rangle$$

We overload Ⓢ to filtering elements from sets of sequences as follows:

$$\begin{aligned} \_ Ⓢ \_ &\in \mathbb{P}(A) \times \mathbb{P}(A^{\omega}) \to \mathbb{P}(A^{\omega}) \\ B Ⓢ S &\overset{\mathsf{def}}{=} \{B Ⓢ s \mid s \in S\} \end{aligned}$$

We also need a projection operator $\Pi_i.s$ that returns the ith element of an n-tuple s understood as a sequence of length n. We define the projection operator formally as:

$$\begin{aligned} &\Pi_{\_}.\_ \in \{1 \ldots n\} \times A^n \to A \\ &\_[\_] \in A^{\omega} \times \mathbb{N}_+ \to A \end{aligned}$$

The projection operator is overloaded to sets of index values as follows.

$$\Pi_{\_}.\_ \in \mathbb{P}(\{1 \ldots n\}) \setminus \emptyset \times A^n \to \bigcup_{1 \le k \le n} A^k$$

$$\begin{aligned} &\Pi_I.s \overset{\mathsf{def}}{=} s' \\ &\quad \text{where } \forall j \in I : \Pi_j.s = \Pi_{\#\{i \in I \mid i \le j\}}.s' \wedge \#s' = \#I \end{aligned}$$

For example we have that:

$$\Pi_{\{1,2\}}.\langle p, q, r\rangle = \langle p, q\rangle$$

For a sequence of tuples s, $\Pi_I.s$ denotes the sequence of k-tuples obtained from s, by projecting each element in s with respect to the index values in I. For example we have that

$$\Pi_{\{1,2\}}.\langle\langle a, r, p\rangle, \langle b, r, p\rangle\rangle = \langle \Pi_{\{1,2\}}.\langle a, r, p\rangle\rangle \frown \langle \Pi_{\{1,2\}}.\langle b, r, p\rangle\rangle = \langle\langle a, r\rangle, \langle b, r\rangle\rangle$$

We define the projection operator on a sequence of n-tuples formally as follows:

$$\Pi_{\_}.\_ \in \mathbb{P}(\{1 \ldots n\}) \setminus \emptyset \times (A^n)^{\omega} \to \bigcup_{1 \le k \le n} (A^k)^{\omega}$$

$$\begin{aligned} &\Pi_I.s \overset{\mathsf{def}}{=} s' \\ &\quad \text{where} \\ &\qquad \forall j \in \{1 \ldots \#s\} : \Pi_I.s[j] = s'[j] \wedge \#s = \#s' \end{aligned}$$

If we want to restrict the view of a sequence of events to only the signals of the events, we may apply the projection operator twice, as follows:

$$\Pi_1.(\Pi_2.\langle !\langle a, r, p, 3\rangle, !\langle b, r, p, 5\rangle\rangle) = \langle\langle a\rangle, \langle b\rangle\rangle$$

Restricting a sequence of events, that is, pairs of kinds and messages, to the second elements of the events yields a sequence of messages. Applying the projection operator a second time with the subscript 1 yields a sequence of signals.

3.4. Traces

A trace t is a sequence of events that fulfils certain well-formedness constraints reflecting the behaviour of the informal model presented in Section 2. We use traces to represent communication histories of components and their interfaces. Hence, the transmitters and consumers in a trace are interfaces. We first formulate two constraints on the timing of events in a trace. The first makes sure that events are ordered by time while the second is needed to avoid Zeno-behaviour. Formally:

$$\forall i, j \in [1..\#t] : i < j \Rightarrow q.t[i] < q.t[j] \tag{8}$$

$$\#t = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t[i] > k \tag{9}$$

For simplicity, we require that two events in a trace never have the same time-stamp. We impose this requirement by assigning each interface a set of time-stamps disjoint from the set of time-stamps assigned to every other interface. Every event of an interface is assigned a unique time-stamp from the set of time-stamps assigned to the interface in question.

The first constraint makes sure that events are totally ordered according to when they take place. The second constraint states that time in an infinite trace always eventually progress beyond any fixed point in time. This implies that time never halts and Zeno-behaviour is therefore not possible. To lift the assumption that two events never happen at the same time, we could replace the current notion of a trace as a sequence of events, to a notion of a trace as a sequence of sets of events where the messages in each set have the same time-stamp.

We also impose a constraint on the ordering of transmission and consumption events in a trace t. According to the operational model a message can be transmitted without being consumed, but it cannot be consumed without having been transmitted. Furthermore, the consumption of messages transmitted to the same party must happen in the same order as transmission. However, since a trace may include consumption events with external transmitters, we can constrain only the consumption of a message from a party which is itself active in the trace. That is, the ordering requirements on t only apply to the communication between the internal parties. This motivates the following formalisation of the ordering constraint:

$$\begin{array}{l}
\mathsf{let}\ N = \{n \in \mathcal{P} \mid \mathsf{rng}.t \cap \mathcal{E}_n \neq \emptyset\} \\
\mathsf{in}\ \ \forall n, m \in N : \\
\quad \mathsf{let}\ i = (\{?\} \times (\mathcal{S} \times n \times m \times \mathcal{Q})) \circledS\, t \\
\qquad\quad o = (\{!\} \times (\mathcal{S} \times n \times m \times \mathcal{Q})) \circledS\, t \\
\quad \mathsf{in}\ \Pi_{\{1,2,3\}}.(\Pi_{\{2\}}.i) \sqsubseteq \Pi_{\{1,2,3\}}.(\Pi_{\{2\}}.o) \wedge \forall j \in \{1..\#i\} : q.o[j] < q.i[j]
\end{array} \tag{10}$$

The first conjunct of constraint (10) requires that the sequence of consumed messages sent from an internal party n to another internal party m, is a prefix of the sequence of transmitted messages from n to m, when disregarding time. We abstract away the timing of events in a trace by applying the projection operator twice. Thus, we ensure that messages communicated between internal parties are consumed in the order they are transmitted. The second conjunct of constraint 10 ensures that for any single message, transmission happens before consumption when both the transmitter and consumer are internal. We let $\mathcal{H}$ denote the set of all traces t that are well-formed with regard to constraints (8), (9) and (10).

3.5. Probabilistic processes

As explained in Section 2.4, we understand the behaviour of an interface as a probabilistic process. The basic mathematical object for representing probabilistic processes is a *probability space* [14, 47]. A probability space is a triple $(\Omega, \mathcal{F}, f)$, where Ω is a sample space, that is, a non-empty set of possible outcomes, $\mathcal{F}$ is a non-empty set of subsets of Ω, and f is a function from $\mathcal{F}$ to $[0, 1]$ that assigns a probability to each element in $\mathcal{F}$.

The set $\mathcal{F}$, and the function f have to fulfil the following constraints: The set $\mathcal{F}$ must be a σ-field over Ω, that is, $\mathcal{F}$ must be not be empty, it must contain Ω and be closed under complement[3] and countable union. The function f must be a *probability measure* on $\mathcal{F}$, that is, a function from $\mathcal{F}$ to $[0, 1]$ such that $f(\emptyset) = 0$, $f(\Omega) = 1$, and for every sequence ω of disjoint sets in $\mathcal{F}$, the following holds: $f(\bigcup_{i=1}^{\#\omega} \omega[i]) = \sum_{i=1}^{\#\omega} f(\omega[i])$ [12]. The last property is referred to as countably additive, or σ-additive.

We represent a probabilistic execution H by a probability space with the set of traces of H as its sample space. If the set of possible traces in an execution is infinite, the probability of a single trace may be zero. To obtain the probability that a certain sequence of events occurs up to a particular point in time, we can look at the probability of the set of all *extensions* of that sequence in a given trace set. Thus, instead of talking of the probability of a single trace, we are concerned with the probability of a set of traces with common prefix, called a *cone*. By $c(t, D)$ we denote the set of all continuations of t in D. For example we have that

$$\begin{aligned} c(\langle a\rangle, \{\langle a, a, b, b\rangle, \langle a, a, c, c\rangle\}) &= \{\langle a, a, b, b\rangle, \langle a, a, c, c\rangle\} \\ c(\langle a, a, b\rangle, \{\langle a, a, b, b\rangle, \langle a, a, c, c\rangle\}) &= \{\langle a, a, b, b\rangle\} \\ c(\langle b\rangle, \{\langle a, a, b, b\rangle, \langle a, a, c, c\rangle\}) &= \emptyset \end{aligned}$$

We define the cone of a finite trace t in a trace set D formally as:

Definition 3.1 (Cone). *Let D be a set of traces. The cone of a finite trace t, with regard to D, is the set of all traces in D with t as a prefix:*

$$\begin{aligned} c\ \_\ \_ &\in \mathcal{H} \times \mathbb{P}(\mathcal{H}) \rightarrow \mathbb{P}(\mathcal{H}) \\ c(t, D) &\overset{\mathsf{def}}{=} \{t' \in D \mid t \sqsubseteq t'\} \end{aligned}$$

We define the *cone set* with regard to a set of traces as:

Definition 3.2 (Cone set). *The cone set of a set of traces D consists of the cones with regard to D of each finite trace that is a prefix of a trace in D:*

$$\begin{aligned} C\_ &\in \mathbb{P}(\mathcal{H}) \rightarrow \mathbb{P}(\mathbb{P}(\mathcal{H})) \\ C(D) &\overset{\mathsf{def}}{=} \{c(t, D) \mid \#t \in \mathbb{N} \wedge \exists t' \in D : t \sqsubseteq t'\} \end{aligned}$$

We understand each trace in the trace set representing a probabilistic process H as a complete history of H. We therefore want to be able to distinguish the state where an execution stops after a given sequence and the state where an execution may continue with different alternatives after the sequence. We say that a finite trace t is complete with regard to a set of traces D if $t \in D$. Let D be a set of set of traces. We define the *complete extension* of the cone set of D as follows:

[3] Note that this is the relative complement with respect to Ω, that is if $A \in \mathcal{F}$, then $\Omega \setminus A \in \mathcal{F}$.

Definition 3.3 (Complete extended cone set). *The complete extended cone set of a set of traces D is the union of the cone set of D and the set of singleton sets containing the finite traces in D:*

$$C_{E\_} \in \mathbb{P}(\mathcal{H}) \rightarrow \mathbb{P}(\mathbb{P}(\mathcal{H}))$$
$$C_E(D) \overset{\mathsf{def}}{=} C(D) \cup \{\{t\} \subseteq D \mid \#t \in \mathbb{N}\}$$

We define a probabilistic execution H formally as:

Definition 3.4 (Probabilistic execution). *A probabilistic execution H is a probability space:*

$$\mathbb{P}(\mathcal{H}) \times \mathbb{P}(\mathbb{P}(\mathcal{H})) \times (\mathbb{P}(\mathcal{H}) \rightarrow [0, 1])$$

whose elements we refer to as D_H, $\mathcal{F}_H$ and f_H where D_H is the set of traces of H, $\mathcal{F}_H$ is the σ-field generated by $C_E(D_H)$, that is the intersection of all σ-fields including $C_E(D_H)$, called the cone-σ-field of D_H, and f_H is a probability measure on $\mathcal{F}_H$.

If D_H is countable then $\mathbb{P}(D_H)$ (the power set of D_H) is the largest σ-field that can be generated from D_H and it is common to define $\mathcal{F}_H$ as $\mathbb{P}(D_H)$. If D_H is uncountable, then, assuming the continuum hypothesis, which states that there is no set whose cardinality is strictly between that of the integers and that of the real numbers, the cardinality of D_H equals the cardinality of the real numbers, and hence of $[0, 1]$. This implies that there are subsets of $\mathbb{P}(D_H)$ which are not measurable, and $\mathcal{F}_H$ is therefore usually a proper subset of $\mathbb{P}(D_H)$ [9]. A simple example of a process with uncountable sample space, is the process that throws a fair coin an infinite number of times [37, 10]. Each execution of this process can be represented by an infinite sequence of zeroes and ones, where 0 represents "head" and 1 represents "tail". The set of infinite sequences of zeroes and ones is uncountable, which can be shown by a diagonalisation argument [5].

3.6. Probabilistic interface execution

We define the set of traces of an interface n as any well-formed trace consisting solely of events where n is the active party. Formally:

$$\mathcal{H}_n \overset{\mathsf{def}}{=} \mathcal{H} \cap {\mathcal{E}_n}^{\omega}$$

We define the behavioural representation of an interface n as a function of its queue history. A queue history of an interface n is a well-formed trace consisting solely of transmission events

$$\langle !m_1, \ldots, !m_k \rangle$$

with n as consumer. That a queue history is well formed implies that the events in the queue history are totally ordered by time. We let $\mathcal{B}_n$ denote the set of queue histories of an interface n. Formally:

$$\mathcal{B}_n \overset{\mathsf{def}}{=} \mathcal{H} \cap \mathcal{E}_n^{\downarrow\omega}$$

A queue history serves as a scheduler for an interface, thereby uniquely determining its behaviour [44, 7]. Hence, a queue history gives rise to a probabilistic execution of an interface. That is, the probabilistic behaviour of an interface n is represented by a function of complete queue histories for n. A *complete queue history* for an interface n records the messages transmitted to n for the whole execution of n, as opposed to a *partial queue history* that records the messages transmitted to n until some (finite) point in time. We define a probabilistic interface execution formally as:

Definition 3.5 (Probabilistic interface execution). *A probabilistic execution of an interface n is a function that for every complete queue history of n returns a probabilistic execution:*

$$I_{n\text{-}} \in \mathcal{B}_n \to \mathbb{P}(\mathcal{H}_n) \times \mathbb{P}(\mathbb{P}(\mathcal{H}_n)) \times (\mathbb{P}(\mathcal{H}_n) \to [0,1])$$ [4]

Hence, $I_n(\alpha)$ denotes the probabilistic execution of n given the complete queue history α. We let $D_n(\alpha), \mathcal{F}_n(\alpha)$ and $f_n(\alpha)$ denote the projections on the three elements of the probabilistic execution of n given queue history α. I.e. $I_n(\alpha) = (D_n(\alpha), \mathcal{F}_n(\alpha), f_N(\alpha))$.

In Section 2 we described how an interface may choose to do nothing. In the denotational trace semantics we represent doing nothing by the empty trace. Hence, given an interface n and a complete queue history α, $D_n(\alpha)$ may consist of only the empty trace, but it may never be empty.

3.6.1. Constraints on interface behaviour

The queue history of an interface represents the input to it from other interfaces. In Section 2.4 we described informally our assumptions about how interfaces interact through queues. In particular, we emphasised that an interface can only consume messages already in its queue, and the same message can be consumed only once. We also assumed that an interface does not send messages to itself. Hence, we require that any $t \in D_n(\alpha)$ fulfils the following constraints:

(11) $\quad \mathsf{let}\ i = (\{?\} \times \mathcal{M}) \circledS t$

$$\mathsf{in}\ \Pi_{\{1,2\}}.(\Pi_{\{2\}}.i) \sqsubseteq \Pi_{\{1,2\}}.(\Pi_{\{2\}}.\alpha) \land \forall j \in \{1..\#i\} : q.\alpha[j] < q.i[j]$$

(12) $\quad \forall j \in [1..\#t] : k.t[j] \neq co.t[j]$

The first conjunct of constraint (11) states that the sequence of consumed messages in t is a prefix of the messages in α, when disregarding time. Thus, we ensure that n only consumes messages it has received in its queue and that they are consumed in the order they arrived. The second conjunct of constraint (11) ensures that messages are only consumed from the queue after they have arrived and with a non-zero delay. Constraint (12) ensures that an interface does not send messages to itself.

A complete queue history of an interface uniquely determines its behaviour. However, we are only interested in capturing time causal behaviour in the sense that the behaviour of an interface at a given point in time should depend only on its input up to and including that point in time and be independent of the content of its queue at any later point.

[4] Note that the type of I_n ensures that for any $\alpha \in \mathcal{B}_n : \mathsf{rng}.\alpha \cap ev.D_n(\alpha) = \emptyset$

In order to formalise this constraint, we first define an operator for truncating a trace at a certain point in time. By $t{\downarrow_k}$ we denote the timed truncation of t, that is, the prefix of t including all events in t with a time-stamp lower than or equal to k. For example we have that:

$$\begin{aligned}
\langle ?\langle c,q,r,1\rangle, !\langle a,r,p,3\rangle, !\langle b,r,p,5\rangle\rangle{\downarrow_4} =& \langle ?\langle c,q,r,1\rangle, !\langle a,r,p,3\rangle\rangle \\
\langle ?\langle c,q,r,1\rangle, !\langle a,r,p,3\rangle, !\langle b,r,p,5\rangle\rangle{\downarrow_8} =& \langle ?\langle c,q,r,1\rangle, !\langle a,r,p,3\rangle, !\langle b,r,p,5\rangle\rangle \\
\langle ?\langle c,q,r,\tfrac{1}{2}\rangle, !\langle a,r,p,\tfrac{3}{2}\rangle, !\langle b,r,p,\tfrac{5}{2}\rangle\rangle{\downarrow_{\frac{3}{2}}} =& \langle ?\langle c,q,r,\tfrac{1}{2}\rangle, !\langle a,r,p,\tfrac{3}{2}\rangle\rangle
\end{aligned}$$

The function $\downarrow$ is defined formally as follows:

$$(13) \qquad \begin{aligned}
&\_{\downarrow}\_ \in \mathcal{H} \times \mathcal{Q} \rightarrow \mathcal{H} \\
&t{\downarrow_k} \overset{\mathsf{def}}{=} \begin{cases} \langle\rangle \text{ if } t = \langle\rangle \vee q.t[1] > k \\ r \text{ otherwise where } r \sqsubseteq t \wedge q.r[\#r] \leq k \\ \qquad\qquad\qquad\qquad \wedge\ (\#r < \#t \Rightarrow q.t[\#r+1] > k) \end{cases}
\end{aligned}$$

We overload the timed truncation operator to sets of traces as follows:

$$\begin{aligned}
&\_{\downarrow}\_ \in \mathbb{P}(\mathcal{H}) \times \mathcal{Q} \rightarrow \mathbb{P}(\mathcal{H}) \\
&S{\downarrow_k} \overset{\mathsf{def}}{=} \{t{\downarrow_k} \mid t \in S\}
\end{aligned}$$

We may then formalise the time causality as follows:

$$\begin{aligned}
\forall \alpha, \beta \in \mathcal{B}_n : \forall q \in \mathcal{Q} : \alpha{\downarrow_q} = \beta{\downarrow_q} \Rightarrow (D_n(\alpha){\downarrow_q} = D_n(\beta){\downarrow_q}) \wedge \\
((\forall t_1 \in D_n(\alpha) : \forall t_2 \in D_n(\beta)) : t_1{\downarrow_q} = t_2{\downarrow_q}) \Rightarrow \\
(f_n(\alpha)(c(t_1{\downarrow_q}, D_n(\alpha))) = f_n(\beta)(c(t_2{\downarrow_q}, D_n(\beta))))
\end{aligned}$$

The first conjunct states that for all queue histories α, β of an interface n, and for all points in time q, if α and β are equal until time q, then the trace sets $D_n(\alpha)$ and $D_n(\beta)$ are also equal until time q. The second conjunct states that if α and β are equal until time q, and we have two traces in $D_n(\alpha)$ and $D_n(\beta)$ that are equal until time q, then the likelihoods of the cones of the two traces truncated at time q in their respective trace sets are equal. Thus, the constraint ensures that the behaviour of an interface at a given point in time depends on its queue history up to and including that point in time, and is independent of the content of its queue history at any later point.

4. Denotational representation of an interface with a notion of risk

Having introduced the underlying semantic model, the next step is to extend it with concepts from risk analysis according to the conceptual model in Figure 3. As already explained, the purpose of extending the semantic model with risk analysis concepts is to represent risks as an integrated part of interface and component behaviour.

4.1. Assets

An *asset* is a physical or conceptual entity which is of value for a stakeholder, that is, for an interface (see Section 2.1) and which the stakeholder wants to protect. We let $\mathcal{A}$ denote the set of all assets and $\mathcal{A}_n$ denote the set of assets of interface n. Note that $\mathcal{A}_n$ may be empty. We require:

$$\forall n, n' \in \mathcal{P} : n \neq n' \Rightarrow \mathcal{A}_n \cap \mathcal{A}_{n'} = \emptyset \tag{14}$$

Hence, assets are not shared between interfaces.

4.2. Incidents and consequences

As explained in Section 2.3 an *incident* is an event that reduces the value of one or more assets. This is a general notion of incident, and of course, an asset may be harmed in different ways, depending on the type of asset. Some examples are reception of corrupted data, transmission of classified data to an unauthorised user, or slow response to a request. We provide a formal model for representing events that harm assets. For a discussion of how to obtain further risk analysis results for components, such as the cause of an unwanted incident, its consequence and probability we refer to [2].

In order to represent incidents formally we need a way to measure harm inflicted upon an asset by an event. We represent the *consequence* of an incident by a positive integer indicating its level of seriousness with regard to the asset in question. For example, if the reception of corrupted data is considered to be more serious for a given asset than the transmission of classified data to an unauthorised user, the former has a greater consequence than the latter with regard to this asset. We introduce a function

$$cv_n\_\_ \in \mathcal{E}_n \times \mathcal{A}_n \rightarrow \mathbb{N} \tag{15}$$

that for an event e and asset a of an interface n, yields the consequence of e to a if e is an incident, and 0 otherwise. Hence, an event with consequence larger than zero for a given asset is an incident with regard to that asset. Note that the same event may be an incident with respect to more than one asset; moreover, an event that is not an incident with respect to one asset, may be an incident with respect to another.

4.3. Incident probability

The *probability* that an incident e occurs during an execution corresponds to the probability of the set of traces in which e occurs. Since the events in each trace are totally ordered by time, and all events include a time-stamp, each event in a trace is unique. This means that a given incident occurs only once in each trace.

We can express the set describing the occurrence of an incident e, in a probabilistic execution H, as $occ(e, D_H)$ where the function occ is formally defined as follows:

$$\begin{aligned} & occ\_\_ \in \mathcal{E} \times \mathbb{P}(\mathcal{H}) \rightarrow \mathbb{P}(\mathcal{H}) \\ & occ(e, D) \overset{\mathsf{def}}{=} \{t \in D \mid e \in \mathsf{rng}.t\} \end{aligned} \tag{16}$$

The set $occ(e, D_H)$ corresponds to the union of all cones $c(t, D_H)$ where e occurs in t (see Section 3.5). Any union of cones can be described as a disjoint set of cones [43]. As described in Section 3, we assume that an interface is assigned at most a countable number of signals and we assume that time-stamps are rational numbers. Hence, it follows that an interface has a countable number of events. Since the set of finite sequences formed from a countable set is countable [25], the union of cones where e occurs in t is countable. Since by definition, the cone-σ-field of an execution H, is closed under countable union, the occurrence of an incident can be represented as a countable union of disjoint cones, that is, it is an element in the cone-σ-field of H and thereby has a measure.

4.4. Risk function

The *risk function* of an interface n takes a consequence, a probability and an asset as arguments and yields a risk value represented by a positive integer. Formally:

$$rf_{n\text{---}} \in \mathbb{N} \times [0,1] \times \mathcal{A}_n \rightarrow \mathbb{N} \tag{17}$$

The risk value associated with an incident e in an execution H, with regard to an asset a, depends on the probability of e in H and its consequence value. We require that

$$rf_n(c,p,a) = 0 \Leftrightarrow c = 0 \vee p = 0$$

Hence, only incidents have a positive risk value, and any incident has a positive risk value.

4.5. Interface with a notion of risk

Putting everything together we end up with the following representation of an interface:

Definition 4.1 (Semantics of an interface). *An interface n is represented by a quadruple*

$$(I_n, \mathcal{A}_n, cv_n, rf_n)$$

consisting of its probabilistic interface execution, assets, consequence function and risk function as explained above.

Given such a quadruple we have the necessary means to calculate the risks associated with an interface for a given queue history. A *risk* is a pair of an incident and its risk value. Hence, for the queue history $\alpha \in \mathcal{B}_n$ and asset $a \in \mathcal{A}_n$ the associated risks are

$$\{rv \mid rv = rf_n(cv(e,a), f_n(occ(e, D_n(\alpha))), a) \wedge rv > 0 \wedge e \in \mathcal{E}_n\}$$

5. Denotational representation of component behaviour

A component is a collection of interfaces, some of which may interact. We may view a single interface as a basic component. A composite component is a component containing at least two interfaces (or basic components). In this section we lift the notion of probabilistic execution from interfaces to components. Furthermore, we explain how we obtain the behaviour of a component from the behaviours of its sub-components. In this section we do not consider the issue of hiding; this is the topic of Section 7.

In Section 5.1 we introduce the notion of conditional probability measure, conditional probabilistic execution and probabilistic component execution. In Section 5.2 we characterise the trace set of a composite component from the trace sets of its sub-components. The cone-σ-field of a probabilistic component execution is generated straightforwardly from that. In Section 5.3 we explain how to define the conditional probability measure for the cone-σ-field of a composite component from the conditional probability measures of its sub-components. Finally, in Section 5.4, we define a probabilistic component execution of a composite component in terms of the probabilistic component executions of its sub-components. We sketch the proof strategies for the lemmas and theorems in this section and refer to Appendix B for the full proofs.

5.1. Probabilistic component execution

The behaviour of a component is completely determined by the set of interfaces it consists of. We identify a component by the set of names of its interfaces. Hence, the behaviour of the component $\{n\}$ consisting of only one interface n, is identical to the behaviour of the interface n. For any set of interfaces N we define:

$$\mathcal{E}_N \overset{\mathsf{def}}{=} \bigcup_{n \in N} \mathcal{E}_n \tag{18}$$

$$\mathcal{E}^{\downarrow}_N \overset{\mathsf{def}}{=} \bigcup_{n \in N} \mathcal{E}^{\downarrow}_n \tag{19}$$

$$\mathcal{H}_N \overset{\mathsf{def}}{=} \mathcal{H} \cap {\mathcal{E}_N}^{\omega} \tag{20}$$

$$\mathcal{B}_N \overset{\mathsf{def}}{=} \mathcal{H} \cap {\mathcal{E}^{\downarrow}_N}^{\omega} \tag{21}$$

Just as for interfaces, we define the behavioural representation of a component N as a function of its queue history. For a single interface a queue history α resolves the external nondeterminism caused by the environment. Since we assume that an interface does not send messages to itself there is no internal non-determinism to resolve. The function representing an interface returns a probabilistic execution which is a probability space. Given an interface n it follows from the definition of a probabilistic execution, that for any queue history $\alpha \in \mathcal{B}_n$, we have $f_n(\alpha)(D_n(\alpha)) = 1$.

For a component N consisting of two or more sub-components, a queue history α must resolve both external and internal non-determinism. For a given queue history α the behaviour of N, is obtained from the behaviours of the sub-components of N that are possible with regard to α. That is, all internal choices concerning interactions between the sub-components of N are fixed by α. This means that the probability of the set of traces of N given a queue history α may be lower than 1, violating the requirement of a probability measure. In order to formally represent the behaviour of a component we therefore introduce the notion of a *conditional probability measure*.

Definition 5.1 (Conditional probability measure). *Let D be a non-empty set and $\mathcal{F}$ be a σ-field over D. A conditional probability measure f on $\mathcal{F}$ is a function that assigns a value in $[0, 1]$ to each element of $\mathcal{F}$ such that; either $f(A) = 0$ for all A in $\mathcal{F}$, or there exists a constant $c \in \langle 0, 1]$*[5] *such that the function f' defined by $f'(A) = f(A)/c$ is a probability measure on $\mathcal{F}$.*

[5] We use $\langle a, b\rangle$ to denote the open interval $\{x \mid a < x < b\}$.

We define a conditional probabilistic execution H formally as:

Definition 5.2 (Conditional probabilistic execution). *A conditional probabilistic execution H is a measure space [14]:*

$$\mathbb{P}(\mathcal{H}) \times \mathbb{P}(\mathbb{P}(\mathcal{H})) \times (\mathbb{P}(\mathcal{H}) \rightarrow [0,1])$$

whose elements we refer to as D_H, $\mathcal{F}_H$ and f_H where D_H is the set of traces of H, $\mathcal{F}_H$ is the cone-σ-field of D_H, and f_H is a conditional probability measure on $\mathcal{F}_H$.

We define a probabilistic component execution formally as:

Definition 5.3 (Probabilistic component execution). *A probabilistic execution of a component N is a function I_N that for every complete queue history of N returns a conditional probabilistic execution:*

$$I_{N}\,\_ \in \mathcal{B}_N \rightarrow \mathbb{P}(\mathcal{H}_N) \times \mathbb{P}(\mathbb{P}(\mathcal{H}_N)) \times (\mathbb{P}(\mathcal{H}_N) \rightarrow [0,1])$$

Hence, $I_N(\alpha)$ denotes the probabilistic execution of N given the complete queue history α. We let $D_N(\alpha), \mathcal{F}_N(\alpha)$ and $f_N(\alpha)$ denote the canonical projections of the probabilistic component execution on its elements.

5.2. Trace sets of a composite component

For a given queue history α, the combined trace sets $D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ and $D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$ such that all the transmission events from N_1 to N_2 are in α and the other way around, constitute the legal set of traces of the composition of N_1 and N_2. Given two probabilistic component executions I_{N_1} and I_{N_2} such that $N_1 \cap N_2 = \emptyset$, for each $\alpha \in \mathcal{B}_{N_1 \cup N_2}$ we define their composite trace set formally as:

$$\begin{aligned}
(22) \qquad & D_{N_1} \otimes D_{N_2}\,\_ \in \mathcal{B}_{N_1 \cup N_2} \rightarrow \mathbb{P}(\mathcal{H}_{N_1 \cup N_2}) \\
& D_{N_1} \otimes D_{N_2}(\alpha) \overset{\mathsf{def}}{=} \\
& \qquad \{t \in \mathcal{H}_{N_1 \cup N_2} | \mathcal{E}_{N_1} \circledS t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_2} \circledS t \in D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha) \wedge \\
& \qquad (\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS \alpha \wedge \\
& \qquad (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha\}
\end{aligned}$$

The definition ensures that the messages from N_2 consumed by N_1 are in the queue history of N_1 and vice versa. The operator $\otimes$ is obviously commutative and also associative since the sets of interfaces of each component are disjoint.

For each $\alpha \in \mathcal{B}_{N_1 \cup N_2}$ the cone-σ-field is generated as before. Hence, we define the cone-σ-field of a composite component as follows:

$$(23) \qquad \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha) \overset{\mathsf{def}}{=} \sigma(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$$

where $\sigma(D)$ denotes the σ-field generated by the set D. We refer to $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as the *composite extended cone set* of $N_1 \cup N_2$.

5.3. Conditional probability measure of a composite component

Consider two components C and O such that $C \cap O = \emptyset$. As described in Section 2, it is possible to decompose a probabilistic choice over actions in such a way that it never involves more than one interface. We may therefore assume that for a given queue history $\alpha \in \mathcal{B}_{C \cup O}$ the behaviour represented by $D_C(\mathcal{E}_C^{\downarrow} \circledS \alpha)$ is independent of the behaviour represented by $D_O(\mathcal{E}_O^{\downarrow} \circledS \alpha)$. Given this assumption the probability of a certain behaviour of the composed component equals the product of the probabilities of the corresponding behaviours of C and O, by the law of statistical independence. As explained in Section 3.5, to obtain the probability that a certain sequence of events t occurs up to a particular point in time in a set of traces D, we can look at the cone of t in D. For a given cone $c \in C_E(D_C \otimes D_O(\alpha))$ we obtain the corresponding behaviours of C and O by filtering c on the events of C and O, respectively.

The above observation with regard to cones does not necessarily hold for all elements of $\mathcal{F}_C \otimes \mathcal{F}_O(\alpha)$. The following simple example illustrates that the probability of an element in $\mathcal{F}_C \otimes \mathcal{F}_O(\alpha)$, which is not a cone, is not necessarily the product of the corresponding elements in $\mathcal{F}_C(\mathcal{E}_C^{\downarrow} \circledS \alpha)$ and $\mathcal{F}_O(\mathcal{E}_O^{\downarrow} \circledS \alpha)$. Assume that the component C tosses a fair coin and that the component O tosses an Othello piece (a disk with a light and a dark face). We assign the singleton time-stamp set $\{1\}$ to C and the singleton time-stamp set $\{2\}$ to O. Hence, the traces of each may only contain one event. For the purpose of readability we represent in the following the events by their signals. The assigned time-stamps ensure that the coin toss represented by the events $\{h, t\}$ comes before the Othello piece toss. We have:

$$\begin{aligned}
D_C(\langle\rangle) &= \{\langle h\rangle, \langle t\rangle\}\\
\mathcal{F}_C(\langle\rangle) &= \{\emptyset, \{\langle h\rangle\}, \{\langle t\rangle\}, \{\langle h\rangle, \langle t\rangle\}\}\\
f_C(\langle\rangle)(\{\langle h\rangle\}) &= 0.5\\
f_C(\langle\rangle)(\{\langle t\rangle\}) &= 0.5\\
&\text{and}\\
D_O(\langle\rangle) &= \{\langle b\rangle, \langle w\rangle\}\\
\mathcal{F}_O(\langle\rangle) &= \{\emptyset, \{\langle b\rangle\}, \{\langle w\rangle\}, \{\langle b\rangle, \langle w\rangle\}\}\\
f_O(\langle\rangle)(\{\langle b\rangle\}) &= 0.5\\
f_O(\langle\rangle)(\{\langle w\rangle\}) &= 0.5
\end{aligned}$$

Let $D_{CO} = D_C \otimes D_O$. The components interacts only with the environment, not with each other. We have:

$$D_{CO}(\langle\rangle) = \{\langle h, b\rangle, \langle h, w\rangle, \langle t, b\rangle, \langle t, w\rangle\}$$

We assume that each element in the sample space (trace set) of the composite component has the same probability. Since the sample space is finite, the probabilities are given by discrete uniform distribution, that is each trace in $D_{CO}(\langle\rangle)$ has a probability of 0.25. Since the traces are mutually exclusive, it follows by the laws of probability that the probability of $\{\langle h, b\rangle\} \cup \{\langle t, w\rangle\}$ is the sum of the probabilities of $\{\langle h, b\rangle\}$ and $\{\langle t, w\rangle\}$, that is 0.5. But this is not the same as $f_C(\langle\rangle)(\{\langle h\rangle, \langle t\rangle\}) \cdot f_O(\langle\rangle)(\{\langle b\rangle, \langle w\rangle\})$[6], which is 1.

[6] We use $\cdot$ to denote normal multiplication.

Since there is no internal communication between C and O, there is no internal non-determinism to be resolved. If we replace the component O with the component R, which simply consumes whatever C transmits, a complete queue history of the composite component reflects only one possible interaction between C and R. Let $D_{CR} = D_C \otimes D_R$. To make visible the compatibility between the trace set and the queue history we include the whole events in the trace sets of the composite component. We have:

$$\begin{aligned} D_{CR}(\langle !\langle h, C, R, 1\rangle\rangle) &= \{\langle !\langle h, C, R, 1\rangle, ?\langle h, C, R, 2\rangle\rangle\} \\ D_{CR}(\langle !\langle t, C, R, 1\rangle\rangle) &= \{\langle !\langle t, C, R, 1\rangle, ?\langle t, C, R, 2\rangle\rangle\} \end{aligned}$$

For a given queue history α, the set $\mathcal{E}_C \circledS D_{CR}(\alpha)$ is a subset of the trace set $D_C(\mathcal{E}_C^{\downarrow} \circledS \alpha)$ that is possible with regard to α (that $\mathcal{E}_C \circledS D_{CR}(\alpha)$ is a subset of $D_C(\mathcal{E}_C^{\downarrow} \circledS \alpha)$ follows from Lemma B.21 which is shown in Appendix B). We call the set of traces of C that are possible with regard to a given queue history α and component R for $CT_{C-R}(\alpha)$, which is short for *conditional traces*.

Given two components N_1 and N_2 and a complete queue history $\alpha \in \mathcal{B}_{N_1 \cup N_2}$, we define the set of conditional traces of N_1 with regard to α and N_2 formally as:

$$\begin{aligned} CT_{N_1 - N_2}(\alpha) \overset{\mathsf{def}}{=} \{t \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) \mid (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq \\ (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha\} \end{aligned} \tag{24}$$

Lemma 5.4. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$CT_{N_1 - N_2}(\alpha) \in \mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) \wedge CT_{N_2 - N_1}(\alpha) \in \mathcal{F}_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS \alpha)$$

Proof sketch: The set $CT_{N_1 - N2}(\alpha)$ includes all traces in $D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$ that are compatible with α, i.e., traces that are prefixes of α when filtered on the transmission events from N_1 to N_2. The key is to show that this set can be constructed as an element in $\mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$. If α is infinite, this set corresponds to the union of (1) all finite traces in $D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$ that are compatible with α and (2) the set obtained by constructing countable unions of cones of traces that are compatible with finite prefixes of $\alpha|_i$ for all $i \in \mathbb{N}$ (where $\alpha|_i$ denotes the prefix of α of length i) and then construct the countable intersection of all such countable unions of cones. If α is finite the proof is simpler, and we do not got into the details here. The same procedure may be followed to show that $CT_{N_2 - N_1}(\alpha) \in \mathcal{F}_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS \alpha)$.

As illustrated by the example above, we cannot obtain a measure on a composite cone-σ-field in the same manner as for a composite extended cone set. In order to define a conditional probability measure on a composite cone-σ-field, we first define a measure on the composite extended cone set it is generated from. We then show that this measure can be uniquely extended to a conditional probability measure on the generated cone-σ-field. Given two probabilistic component executions I_{N_1} and I_{N_2} such that $N_1 \cap N_2 = \emptyset$, for each $\alpha \in \mathcal{B}_{N_1 \cup N_2}$ we define a measure $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ on $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ formally as follows:

$$\begin{aligned} &\mu_{N_1} \otimes \mu_{N_2\,\text{--}} \in \mathcal{B}_{N_1 \cup N_2} \rightarrow (C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \rightarrow [0,1]) \\ &\mu_{N_1} \otimes \mu_{N_2}(\alpha)(c) \overset{\mathsf{def}}{=} f_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)(\mathcal{E}_{N_1} \circledS c) \cdot f_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS \alpha)(\mathcal{E}_{N_2} \circledS c) \end{aligned} \tag{25}$$

Theorem 5.5. *The function $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ is well defined.*

Proof sketch: For any $c \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ we must show that $(\mathcal{E}_{N_1} \circledS c) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ and $(\mathcal{E}_{N_2} \circledS c) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$. If c is a singleton (containing exactly one trace) the proof follows from the fact that (1): if $(D, \mathcal{F}, f)$ is a conditional probabilistic execution and t is a trace in D, then $\{t\} \in \mathcal{F}$ [37], and (2): that we can show $\mathcal{E}_{N_1} \circledS t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_2} \circledS t \in D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$ from Definition 3.3 and definition (22).

If c is a cone $c(t, D_{N_1} \otimes D_{N_2}(\alpha))$ in $C(D_{N_1} \otimes D_{N_2}(\alpha))$, we show that $CT_{N_1 - N_2}(\alpha)$, intersected with $c(\mathcal{E}_{N_1} \circledS t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$ and the traces in $D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ that are compatible with t with regard to the timing of events, is an element of $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ that equals $(\mathcal{E}_{N_1} \circledS c)$. We follow the same procedure to show that $(\mathcal{E}_{N_2} \circledS c) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$.

Lemma 5.6. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let $\mu_{N_1} \otimes \mu_{N_2}$ be a measure on the extended cones set of $D_{N_1} \otimes D_{N_2}$ as defined by (25). Then, for all complete queue histories $\alpha \in \mathcal{B}_{N_1 \cup N_2}$*

1. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\emptyset) = 0$
2. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ *is σ-additive*
3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

Proof sketch: We sketch the proof strategy for point 2 of Lemma 5.6. The proofs of point 1 and 3 are simpler, and we do not go into the details here. Assume ϕ is a sequence of disjoint sets in $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$. We construct a sequence ψ of length $\#\phi$ such that $\forall i \in [1..\#\phi] : \psi[i] = \{(\mathcal{E}_{N_1} \circledS t, \mathcal{E}_{N_2} \circledS t) \mid t \in \phi[i]\}$ and show that $\bigcup_{i=1}^{\#\psi} \psi[i] = \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]$. It follows by Theorem 5.5 that $(\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) \times (\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i])$ is a measurable rectangle [14] in $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \times \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$. From the above, and the product measure theorem [14] it can be shown that $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) = \sum_{i=1}^{\#\phi} f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$ $(\mathcal{E}_{N_2} \circledS \phi[i])$.

Theorem 5.7. *There exists a unique extension of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to the cone-σ-field $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.*

Proof sketch: We extend $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ in a stepwise manner to a set obtained by first adding all complements of the elements in $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$, then adding the finite intersections of the new elements and finally adding finite unions of disjoint elements. For each step we extend $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ and show that the extension is σ-additive. We end up with a finite measure on the field generated by $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$. By the extension theorem [14] it follows that this measure can be uniquely extended to a measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.

Corollary 5.8. *Let $f_{N_1} \otimes f_{N_2}(\alpha)$ be the unique extension of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to the cone-σ-field $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$. Then $f_{N_1} \otimes f_{N_2}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.*

Proof sketch: We first show that $f_{N_1} \otimes f_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$. When $f_{N_1} \otimes f_{N_2}(\alpha)$ is a measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$ such that $f_{N_1} \otimes f_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$ we can show that $f_{N_1} \otimes f_{N_2}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.

5.4. Composition of probabilistic component executions

We may now lift the $\otimes$-operator to probabilistic component executions. Let I_{N_1} and I_{N_2} be probabilistic component executions such that $N_1 \cap N_2 = \emptyset$. For any $\alpha \in \mathcal{B}_{N_1 \cup N_2}$ we define:

$$I_{N_1} \otimes I_{N_2}(\alpha) \overset{\mathsf{def}}{=} (D_{N_1} \otimes D_{N_2}(\alpha), \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha), f_{N_1} \otimes f_{N_2}(\alpha)) \tag{26}$$

where $f_{N_1} \otimes f_{N_2}(\alpha)$ is defined to be the unique extension of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.

Theorem 5.9. *$I_{N_1} \otimes I_{N_2}$ is a probabilistic component execution of $N_1 \cup N_2$.*

Proof sketch: This can be shown from definitions (22) and (23) and Corollary 5.8.

6. Denotational representation of a component with a notion of risk

For any disjoint set of interfaces N we define:

$$A_N \overset{\mathsf{def}}{=} \bigcup_{n \in N} A_n$$
$$cv_N \overset{\mathsf{def}}{=} \bigcup_{n \in N} cv_n$$
$$\mathit{rf}_N \overset{\mathsf{def}}{=} \bigcup_{n \in N} \mathit{rf}_n$$

The reason why we can take the union of functions with disjoint domains is that we understand a function as a set of *maplets*. A maplet is a pair of two elements corresponding to the argument and the result of a function. For example the following set of three maplets

$$\{(e_1 \mapsto f(e_1)), (e_2 \mapsto f(e_2)), (e_2 \mapsto f(e_2))\}$$

characterises the function $f \in \{e_1, e_2, e_3\} \to S$ uniquely. The arrow $\mapsto$ indicates that the function yields the element to the right when applied to the element to the left [3].

We define the semantic representation of a component analogous to that of an interface, except that we now have a set of interfaces N, instead of a single interface n:

Definition 6.1 (Semantics of a component). *A component is represented by a quadruple*

$$(I_N, A_N, cv_N, \mathit{rf}_N)$$

consisting of its probabilistic component execution, its assets, consequence function and risk function, as explained above.

We define composition of components formally as:

Definition 6.2 (Composition of components). *Given two components N_1 and N_2 such that $N_1 \cap N_2 = \emptyset$. We define their composition $N_1 \otimes N_2$ by*

$$(I_{N_1} \otimes I_{N_2}, A_{N_1} \cup A_{N_2}, cv_{N_1} \cup cv_{N_2}, \mathit{rf}_{N_1} \cup \mathit{rf}_{N_2})$$

7. Hiding

In this section we explain how to formally represent hiding in a denotational semantics with risk. As explained in Section 2.5 we must take care not to hide incidents that affect assets belonging to externally observable interfaces, when we hide internal interactions. An interface is externally observable if it interacts with interfaces in the environment. We define operators for hiding assets and interface names from a component name and from the semantic representation of a component. The operators are defined in such a way that partial hiding of internal interaction is allowed. Thus internal events that affect assets belonging to externally observable interfaces may remain observable after hiding. Note that hiding of assets and interface names is optional. The operators defined below simply makes it possible to hide e.g. all assets belonging to a certain interface n, as well as all events in an execution where n is the active party. We sketch the proof strategies for the lemmas and theorems in this section and refer to Appendix B for the full proofs.

Until now we have identified a component by the set of names of its interfaces. This has been possible because an interface is uniquely determined by its name, and the operator for composition is both associative and commutative. Hence, until now it has not mattered in which order the interfaces and resulting components have been composed. When we in the following introduce two hiding operators this becomes however an issue. For example, consider a component identified by

$$N \overset{\mathsf{def}}{=} \{c_1, c_2, c_3\}$$

Then we need to distinguish the component $\delta c_2 : N$, obtained from N by hiding interface c_2, from the component

$$\{c_1, c_3\}.$$

To do that we build the hiding information into the name of a component obtained with the use of hiding operators. A component name is from now one either

(a) a set of interface names,

(b) of the form $\delta n : N$ where N is a component name and n is an interface name,

(c) of the form $\sigma a : N$ where N is a component name and a is an asset, or

(d) of the form $N_1 +\!\!+ N_2$ where N_1 and N_2 are component names and at least one of N_1 or N_2 contains a hiding operator.

Since we now allow hiding operators in component names we need to take this into consideration when combining them. We define a new operator for combining two component names N_1 and N_2 as follows:

$$(27) \qquad N_1 \uplus N_2 \overset{\mathsf{def}}{=} \begin{cases} N_1 \cup N_2 \text{ if neither } N_1 \text{ nor } N_2 \text{ contain hiding operators} \\ N_1 +\!\!+ N_2 \text{ otherwise} \end{cases}$$

By $\mathsf{in}(N)$ we denote the set of all hidden and not hidden interface names occurring in the component name N. We generalise definitions (18) to (21) to component names with hidden assets and interface names as follows:

$$\begin{array}{lll}
(28) & \mathcal{E}_{\sigma a\,:\,N} \overset{\mathsf{def}}{=} \mathcal{E}_{N} & \mathcal{E}_{\delta n\,:\,N} \overset{\mathsf{def}}{=} \mathcal{E}_{\mathsf{in}(N)\setminus\{n\}} \\
(29) & \mathcal{E}^{\downarrow}_{\sigma a\,:\,N} \overset{\mathsf{def}}{=} \mathcal{E}^{\downarrow}_{N} & \mathcal{E}^{\downarrow}_{\delta n\,:\,N} \overset{\mathsf{def}}{=} \mathcal{E}^{\downarrow}_{\mathsf{in}(N)\setminus\{n\}} \\
(30) & \mathcal{H}_{\sigma a\,:\,N} \overset{\mathsf{def}}{=} \mathcal{H} \cap \mathcal{E}_{\sigma a\,:\,N}{}^{\omega} & \mathcal{H}_{\delta n\,:\,N} \overset{\mathsf{def}}{=} \mathcal{H} \cap \mathcal{E}_{\delta n\,:\,N}{}^{\omega} \\
(31) & \mathcal{B}_{\sigma a\,:\,N} \overset{\mathsf{def}}{=} \mathcal{B}_{N} & \mathcal{B}_{\delta n\,:\,N} \overset{\mathsf{def}}{=} ((\mathcal{E}_{\overline{\mathsf{in}(N)}} \setminus \mathcal{E}^{\downarrow}_{n}) \cup \mathcal{E}_{\mathsf{in}(N)}) \circledS \mathcal{B}_{N}
\end{array}$$

Definition 7.1 (Hiding of interface in a probabilistic component execution). *Given an interface name n and a probabilistic component execution I_N we define:*

$$\begin{array}{rrl}
 & \delta n : I_N(\alpha) & \overset{\mathsf{def}}{=} (D_{\delta n\,:\,N}(\alpha), \mathcal{F}_{\delta n\,:\,N}(\alpha), f_{\delta n\,:\,N}(\alpha)) \\
\textit{where} & D_{\delta n\,:\,N}(\alpha) & \overset{\mathsf{def}}{=} \{\mathcal{E}_{\delta n\,:\,N} \circledS t \mid t \in D_N(\delta n : \alpha)\} \\
 & \mathcal{F}_{\delta n\,:\,N}(\alpha) & \overset{\mathsf{def}}{=} \sigma(C_E(D_{\delta n\,:\,N}(\alpha))) \textit{ i.e., the cone-}\sigma\textit{-field of } D_{\delta n\,:\,N}(\alpha) \\
 & f_{\delta n\,:\,N}(\alpha)(c) & \overset{\mathsf{def}}{=} f_N(\delta n : \alpha)\big(\{t \in D_N(\delta n : \alpha) \mid \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\}\big) \\
 & \delta n : \alpha & \overset{\mathsf{def}}{=} \big((\mathcal{E}_{\overline{\mathsf{in}(N)}} \setminus \mathcal{E}^{\downarrow}_{n}) \cup \mathcal{E}_{\mathsf{in}(N)}\big) \circledS \alpha
\end{array}$$

When hiding an interface name n from a queue history α, as defined in the last line of Definition 7.1, we filter away the external input to n but keep all internal transmissions, including those sent to n. This is because we still need the information about the internal interactions involving the hidden interface to compute the probability of interactions it is involved in, after the interface is hidden from the outside.

Lemma 7.2. *If I_N is a probabilistic component execution and n is an interface name, then $\delta n : I_N$ is a probabilistic component execution.*

Proof sketch: We must show that: (1) $D_{\delta n\,:\,N}(\alpha)$ is a set of well-formed traces; (2) $\mathcal{F}_{\delta n:N}(\alpha)$ is the cone-σ-field of $D_{\delta n\,:\,N}(\alpha)$; and (3) $f_{\delta n\,:\,N}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{\delta n\,:\,N}(\alpha)$. (1) If a trace is well-formed it remains well-formed after filtering away events with the hiding operator, since hiding interface names in a trace does not affect the ordering of events. The proof of (2) follows straightforwardly from Definition 7.1.

In order to show (3), we first show that $f_{\delta n\,:\,N}(\alpha)$ is a measure on $\mathcal{F}_{\delta n\,:\,N}(\alpha)$. In order to show this, we first show that the function $f_{\delta n\,:\,N}$ is well defined. I.e., for any $c \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$ we show that $\big\{t \in D_N(\delta n : \alpha) \mid \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\big\} \in \mathcal{F}_N(\delta n : \alpha)$. We then show that $f_N(\delta n : \alpha)(\emptyset) = 0$ and that $f_N(\delta n : \alpha)$ is σ-additive. Secondly, we show that $f_{\delta n\,:\,N}(\alpha)(D_{\delta n\,:\,N}(\alpha)) \leq 1$. When $f_{\delta n\,:\,N}(\alpha)$ is a measure on $\mathcal{F}_{\delta n\,:\,N}(\alpha)$ such that $f_{\delta n\,:\,N}(\alpha)(D_{\delta n\,:\,N}(\alpha)) \leq 1$ we can show that $f_{\delta n\,:\,N}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{\delta n\,:\,N}(\alpha)$.

Definition 7.3 (Hiding of component asset). *Given an asset a and a component*

(I_N, A_N, cv_N, rf_N) *we define:*

$$\begin{aligned} \sigma a:(I_N, A_N, cv_N, rf_N) &\overset{\mathsf{def}}{=} (I_N, \sigma a : A_N, \sigma a : cv_N, \sigma a : rf_N) \\ \textit{where} \quad \sigma a : A_N &\overset{\mathsf{def}}{=} A_N \setminus \{a\} \\ \sigma a : cv_N &\overset{\mathsf{def}}{=} cv_N \setminus \{(e, a) \mapsto c \mid e \in \mathcal{E} \wedge c \in \mathbb{N}\} \\ \sigma a : rf_N &\overset{\mathsf{def}}{=} rf_N \setminus \{(c, p, a) \mapsto r \mid c, r \in \mathbb{N} \wedge p \in [0, 1]\} \end{aligned}$$

As explained in Section 6 we see a function as a set of maplets. Hence, the consequence and risk function of a component with asset a hidden is the set-difference between the original functions and the set of maplets that has a as one of the parameters of its first element.

Theorem 7.4. *If N is a component and a is an asset, then $\sigma a : N$ is a component.*

Proof sketch: This can be shown from Definition 7.3 and Definition 6.1.

We generalise the operators for hiding interface names and assets to the hiding of sets of interface names and sets of assets in the obvious manner.

Definition 7.5 (Hiding of component interface). *Given an interface name n and a component (I_N, A_N, cv_N, rf_N) we define:*

$$\delta n :(I_N, A_N, cv_N, rf_N) \overset{\mathsf{def}}{=} (\delta n : I_N, \sigma A_n : A_N, \sigma A_n : cv_N, \sigma A_n : rf_N)$$

Theorem 7.6. *If N is a component and n is an interface name, then $\delta n : N$ is a component.*

Proof sketch: This can be show from Lemma 7.2 and Theorem 7.4.

Since, as we have shown above, components are closed under hiding of assets and interface names, the operators for composition of components, defined in Section 5, are not affected by the introduction of hiding operators. We impose the restriction that two components can only be composed by ⊗ if their sets of interface names are disjoint, independent of whether they are hidden or not.

8. Related work

In this section we place our work in relation to ongoing research within related areas such as security modelling and approaches to representing probabilistic components. We also relate our component model to a taxonomy of component models [28].

8.1. Security modelling

There are a number of proposals to integrate security requirements into the requirements specification, such as SecureUML and UMLsec. SecureUML [32] is a method for modelling access control policies and their integration into model-driven software development. SecureUML is based on role-based access control and specifies security requirements for well-behaved applications in predictable environments. UMLsec [19] is an extension to UML that enables the modelling of security-related features such as confidentiality and access control. Neither of these two approaches have particular focus on component-oriented specification.

Khan and Han [22] characterise security properties of composite systems, based on a security characterisation framework for basic components [23, 20, 21]. They define a *compositional security contract* CsC for two components, which is based on the compatibility between their required and ensured security properties. They also give a guideline for constructing system level contracts, based on several CsCs. This approach has been designed to capture security properties, while our focus is on integrating risks into the semantic representation of components.

8.2. Probabilistic components

In order to model systems that are both reactive and probabilistic the external nondeterminism caused by the environment must be resolved. Our idea to use queue histories to resolve the external nondeterminism of probabilistic components is inspired by the use of schedulers, also known as adversaries, which is a common way to resolve external nondeterminism in reactive systems [8, 44, 7]. A scheduler specifies how to choose between nondeterministic alternatives.

Segala and Lynch [44, 43] use a randomised scheduler to model input from an external environment and resolve the nondeterminism of a probabilistic I/O automaton. They define a probability space [9] for each probabilistic execution of an automaton, given a scheduler.

Alfaro et al. [7] present a probabilistic model for variable-based systems with trace semantics similar to that of Segala and Lynch. They define a trace as a sequence of states, and a state as an assignment of values to a set of variables. Each component has a set of controlled variables and a set of external variables. Alfaro et al. represent a system by a set of probability distributions on traces, called bundles. They use schedulers to choose the initial and updated values for variables. Unlike the model of Segala and Lynch, their allows multiple schedulers to resolve the nondeterminism of each component. The key idea is to have separate schedulers for the controlled and external variables to ensure that variable behaviours are probabilistically independent. According to Alfaro et al. this ensures so called *deep compositionality* of their system model.

In a system model with deep compositionality the semantics of a composite system can be obtained from the semantics of its constituents. In contrast, shallow compositionality provides the means to specify composite components syntactically [7]. The semantics of a composite specification is obtained from the syntactic composite specification, but the semantics of this composition is not directly related to that of its constituents.

Seidel uses a similar approach in her extension of CSP with probabilities [45]. Internal nondeterministic choice is replaced by probabilistic choice. A process is represented by a conditional probability measure that, given a trace produced by the environment, returns a probability distribution over traces.

An alternative approach to handle external nondeterminism in probabilistic, reactive systems is to treat the assignment of probabilities of alternative choices as a refinement. This approach is used for example in probabilistic action systems [46, 52], where nondeterministic choices are replaced by probabilistic choices. A nondeterministic action system is transformed to a (deterministic) probabilistic system through the distribution of probabilistic information over alternative behaviours.

Our decision to use a cone-based probability space to represent probabilistic systems is inspired by the work on probabilistic I/O automata [44, 43] by Segala and Lynch and probabilistic sequence diagrams (pSTAIRS) [38, 37] by Refsdal. Segala uses probability spaces whose σ-fields are cone-σ-fields to represent fully probabilistic automata, that is, automata with probabilistic choice but without non-determinism. In pSTAIRS [37] the ideas of Segala and Lynch is applied to the trace-based semantics of STAIRS [15, 42, 41]. A probabilistic system is represented as a probability space where the σ-field is generated from a set of cones of traces describing component interactions. In pSTAIRS all choices (nondeterministic, mandatory and probabilistic) are global, that is, the different types of choices may only be specified for closed systems, and there is no nondeterminism stemming from external input.

Since we wish to represent the behaviour of a component independently of its environment we cannot use global choice operators of the type used in pSTAIRS. We build upon the work of pSTAIRS and extend its probabilistic model to open, reactive components. We define probabilistic choice at the level of individual component interfaces and use queue histories to resolve external nondeterminism. Hence, we represent a probabilistic component execution as a function of queue histories, instead of by a single probability space.

8.3. Component models

Lau and Wang [28] have surveyed current component models and classified them into a taxonomy based on commonly accepted criteria for successful component-based development [28]. According to the criteria components should be pre-existing reusable software units which developers can reuse to compose software for different applications. Furthermore components should be composable into composite components which, in turn, can be composed with (composite) components into even larger composites, and so on. These criteria necessitate the use of a repository in the design phase. It must be possible to deposit and retrieve composites from a repository, just like any components.

Lau and Wang [28] divide current component models into four categories based on their facilities for composition during the various phases of a component life cycle. According to their evaluation, no current component model provides mechanisms for composition in all phases. They propose a component model with explicitly defined component connectors, to ensure encapsulation of control, thereby facilitating compositionality during all phases of development.

Our component model is purely semantic. It can be used to represent component implementations. We have at this point not defined a syntax for specifying components. The purpose of the presented component model is to form the necessary basis for building applied tools and methods for component-based risk analysis. Current approaches to specifying probabilistic components, discussed in Section 8.2, can be used as a basis for a specification language needed in such a method.

9. Conclusion

We have presented a component model that integrates component risks as part of the component behaviour. The component model is meant to serve as a formal basis for component-based risk analysis. To ensure modularity of our component model we represent a stakeholder by the component interface, and identify assets on behalf of component interfaces. Thus we avoid referring to concepts that are external to a component in the component model

In order to model the probabilistic aspect of risk, we represent the behaviour of a component by a probability distribution over traces. We use queue histories to resolve both internal and external non-determinism. The semantics of a component is the set of probability spaces given all possible queue histories of the component.

We define composition in a fully compositional manner: The semantics of a composite component is completely determined by the semantics of its constituents. Since we integrate the notion of risk into component behaviour, we obtain the risks of a composite component by composing the behavioural representations of its sub-components.

The component model provides a foundation for component-based risk analysis, by conveying how risks manifests themselves in an underlying component implementation. By component-based risk analysis we mean that risks are identified, analysed and documented at the component level, and that risk analysis results are composable.

Our semantic model is not tied to any specific syntax or specification technique. At this point we have no compliance operator to check whether a given component implementation complies with a component specification. In order to be able to check that a component implementation fulfils a requirement to protection specification we would like to define a compliance relation between specifications in STAIRS, or another suitable specification language, and components represented in our semantic model.

We believe that a method for component-based risk analysis will facilitate the integration of risk analysis into component-based development, and thereby make it easier to predict the effects on component risks caused by upgrading or substituting sub-parts.

Acknowledgements

The research presented in this report has been partly funded by the Research Council of Norway through the research projects COMA 160317 (Component-oriented model-based security analysis) and DIGIT 180052/S10 (Digital interoperability with trust), and partly by the EU 7th Research Framework Programme through the Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS).

We would like to thank Bjarte M. Østvold for creating lpchk: a proof analyser for proofs written in Lamport's style [27] that checks consistency of step labelling and performs parentheses matching, and also for proof reading and useful comments.

References

[1] V. I. Bogachev. *Measure theory*, volume 1. Springer, 2007.

[2] G. Brændeland and K. Stølen. Using model-driven risk analysis in component-based development. In *Dependability and Computer Engineering: Concepts for Software-Intensive Systems.* IGI Global, 2011.

[3] M. Broy and K. Stølen. *Specification and development of interactive systems – Focus on streams, interfaces and refinement.* Monographs in computer science. Springer, 2001.

[4] J. Cheesman and J. Daniels. *UML Components. A simple process for specifying component-based software.* Component software series. Addison-Wesley, 2001.

[5] R. Courant and H. Robbins. *What Is Mathematics? An Elementary Approach to Ideas and Methods.* Oxford University Press, 1996.

[6] I. Crnkovic and M. Larsson. *Building reliable component-based software systems.* Artech-House, 2002.

[7] L. de Alfaro, T. A. Henzinger, and R. Jhala. Compositional methods for probabilistic systems. In *CONCUR '01: Proceedings of the 12th International Conference on Concurrency Theory*, pages 351–365. Springer-Verlag, 2001.

[8] C. Derman. *Finite state Markovian decision process*, volume 67 of *Mathematics in science and engineering*. Academic Press, 1970.

[9] R. M. Dudley. *Real analysis and probability.* Cambridge studies in advanced mathematics. Cambridge, 2002.

[10] Probability theory. Encyclopædia Britannica Online, 2009.

[11] D. G. Firesmith. Engineering safety and security related requirements for software intensive systems. *International Conference on Software Engineering Companion*, 0:169, 2007.

[12] G. B. Folland. *Real Analysis: Modern Techniques and Their Applications.* Pure and Applied Mathematics. John Wiley and Sons Ltd (USA), 2nd edition, 1999.

[13] P. Halmos and S. Givant. *Introduction to Boolean Algebras*, chapter Infinite operations, pages 45–52. Undergraduate Texts in Mathematics. Springer, 2009.

[14] P. R. Halmos. *Measure Theory.* Springer-Verlag, 1950.

[15] Ø. Haugen and K. Stølen. STAIRS – Steps to Analyze Interactions with Refinement Semantics. In *Proceedings of the Sixth International Conference on UML (UML'2003)*, volume 2863 of *Lecture Notes in Computer Science*, pages 388–402. Springer, 2003.

[16] J. He, M. Josephs, and C. A. R. Hoare. A theory of synchrony and asynchrony. In *IFIP WG 2.2/2.3 Working Conference on Programming Concepts and Methods*, pages 459–478. North Holland, 1990.

[17] ISO. *Risk management – Vocabulary*, 2009. ISO Guide 73:2009.

[18] ISO/IEC. *Information Technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*, 2004. ISO/IEC 13335-1:2004.

[19] J. Jürjens, editor. *Secure systems development with UML.* Springer, 2005.

[20] K. M. Khan and J. Han. Composing security-aware software. *IEEE Software*, 19(1):34–41, 2002.

[21] K. M. Khan and J. Han. A process framework for characterising security properties of component-based software systems. In *Australian Software Engineering Conference*, pages 358–367. IEEE Computer Society, 2004.

[22] K. M. Khan and J. Han. Deriving systems level security properties of component based composite systems. In *Australian Software Engineering Conference*, pages 334–343, 2005.

[23] K. M. Khan, J. Han, and Y. Zheng. A framework for an active interface to characterise compositional security contracts of software components. In *Australian Software Engineering Conference*, pages 117–126, 2001.

[24] A. N. Kolomogorov and S. V. Fomin. *Introductory real analysis.* Prentice-Hall, 1970.

[25] P. Komjáth and V. Totik. *Problems and theorems in classical set theory.* Problem books in mathematics. Springer, 2006.

[26] H. Kooka and P. W. Daly. *Guide to LaTeX.* Addison-Wesley, 4th edition, 2003.

[27] L. Lamport. How to write a proof. *American Mathematical Monthly*, 102(7):600–608, 1993.

[28] K.-K. Lau and Z. Wang. Software component models. *IEEE Transactions on software engineering*, 33(10):709–724, 2007.

[29] K. T. Leung and D. L. C. Chen. *Elementary set theory.* Hong Kong University press, 8th edition, 1991.

[30] N. G. Leveson. *Safeware: System Safety and Computers.* ACM Press, New York, NY, USA, 2001.

[31] B. Liu. *Uncertainty Theory.* Studies in fuzziness and soft computing. Springer, 2nd edition, 2007.

[32] T. Lodderstedt, D. A. Basin, and J. Doser. SecureUML: A UML-based modeling language for model-driven security. In *Proceedings of the 5th International Conference, UML 2002 – The Unified Modeling Language*, volume 2460 of *Lecture Notes in Computer Science*, pages 426–441. Springer, 2002.

[33] G. McGraw. *Sofware security: Building security in.* Software Security Series. Adison-Wesley, 2006.

[34] S. Meyn. *Control Techniques for Complex Networks.* Cambridge University Press, 2007.

[35] S. Negri and J. von Plato. *Structural Proof Theory.* Cambridge University Press, 2001.

[36] D. S. Platt. *Introducing Microsoft .NET.* Microsoft Press International, 2001.

[37] A. Refsdal. *Specifying Computer Systems with Probabilistic Sequence Diagrams.* PhD thesis, Faculty of Mathematics and Natural Sciences, University of Oslo, 2008.

[38] A. Refsdal, R. K. Runde, and K. Stølen. Underspecification, inherent nondeterminism and probability in sequence diagrams. In *Proceedings of the 8th IFIP International Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS'2006)*, volume 4037 of *Lecture Notes in Computer Science*, pages 138–155. Springer, 2006.

[39] E. Roman, R. P. Sriganesh, and G. Brose. *Mastering Enterprise JavaBeans*. Wiley, 3rd edition, 2006.

[40] J. Rumbaugh, I. Jacobsen, and G. Booch. *The unified modeling language reference manual*. Addison-Wesley, 2005.

[41] R. K. Runde. *STAIRS - Understanding and Developing Specifications Expressed as UML Interaction Diagrams*. PhD thesis, Faculty of Mathematics and Natural Sciences, University of Oslo, 2007.

[42] R. K. Runde, Ø. Haugen, and K. Stølen. The Pragmatics of STAIRS. In *4th International Symposium, Formal Methods for Components and Objects (FMCO 2005)*, volume 4111 of *Lecture Notes in Computer Science*, pages 88–114. Springer, 2006.

[43] R. Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD thesis, Laboratory for Computer Science, Massachusetts Institute of Technology, 1995.

[44] R. Segala and N. A. Lynch. Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing*, 2(2):250–273, 1995.

[45] K. Seidel. Probabilistic communicationg processes. *Theoretical Computer Science*, 152(2):219–249, 1995.

[46] K. Sere and E. Troubitsyna. Probabilities in action system. In *Proceedings of the 8th Nordic Workshop on Programming Theory*, 1996.

[47] A. V. Skorokhod. *Basic principles and application of probability theory*. Springer, 2005.

[48] Standards Australia, Standards New Zealand. *Australian/New Zealand Standard. Risk Management*, 2004. AS/NZS 4360:2004.

[49] C. Szyperski and C. Pfister. Workshop on component-oriented programming. In M. Mülhauser, editor, *Special Issues in Object-Oriented Programming – ECOOP'96 Workshop Reader*, pages 127–130. dpunkt Verlag, 1997.

[50] A. J. Townsend. *Functions Of A Complex Variable*. BiblioLife, 2009. First published by Cornwell University Library in 1915.

[51] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge tracts in theoretical computer science. Cambridge University Press, 2nd edition, 2000.

[52] E. Troubitsyna. Reliability assessment through probabilistic refinement. *Nordic Journal of Computing*, 6(3):320–342, 1999.

[53] D. Verdon and G. McGraw. Risk analysis in software design. *IEEE Security & Privacy*, 2(4):79–84, 2004.

[54] E. W. Weisstein. *CRC Concise Encyclopedia of Mathematics*. Chapmand & Hall/CRC, 2nd edition, 2002.

A. Auxiliary definitions

Here is a summary of the definitions we use to prove the results in Appendix B.

A.1. Sets

We use $\mathbb{N}$ to denote the set of *natural numbers*:

$$\mathbb{N} \overset{\mathsf{def}}{=} \{0, 1, 2, 3, \ldots, n, n+1, \ldots\}$$

and $\mathbb{N}_+$ to denote the set of strictly positive natural numbers:

$$\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$$

The cross product of two sets A and B, denoted $A \times B$, is the set of all pairs where the first element is in A and the second element is in B. Formally,

$$A \times B \overset{\mathsf{def}}{=} \{(a, b) \mid a \in A, b \in B\} \tag{32}$$

A.2. Logic

We sometimes use let statements in order to make substitution in logical formulas more readable. Any let statement is on the following form

$$\begin{array}{ll}\mathsf{let} & v_1 = e_1 \\ & \vdots \\ & v_n = e_n \\ \mathsf{in} & P\end{array}$$

where $v_1, \ldots, v_n$ are logical variables, $e_1, \ldots, e_n$ are expressions, and P is a formula. We require that the variables are distinct

$$j \neq k \Rightarrow v_j \neq v_k$$

and that v_j is not free in the expression e_k if $k \leq j$. The let statement can be understood as a shorthand for the formula

$$\exists v_1, \ldots, v_n : v_1 = e_1 \wedge \cdots \wedge v_n = e_n \wedge P$$

We often use where to introduce auxiliary identifiers $v_1, \ldots, v_n$. The where statement is of the form

$$P_1 \quad \mathsf{where} \quad v_1, \ldots, v_n \ \mathsf{so\ that} \quad P_2$$

where $v_1, \ldots, v_n$ are logical variables and P_1, P_2 are formulas. It can be understood as a shorthand for the formula

$$\exists v_1, \ldots, v_n : P_1 \wedge P_2$$

A.3. Probability theory

We introduce some basic concepts from measure theory [14, 12, 9, 31] that we use to define probabilistic executions.

Definition A.1 (Countable set). *A set is countable if its elements can be arranged into a finite or infinite sequence [25].*

Definition A.2 (Countably additive function). *A function f on a set D is countably additive (also referred to as σ-additive) if for every sequence ω of disjoint sets in D whose union is also in D we have*

$$f(\bigcup_{i=1}^{\#\omega} \omega[i]) = \sum_{i=1}^{\#\omega} f(\omega[i])$$

Definition A.3 (Field). *Given a set D, a collection $\mathcal{F} \subset \mathbb{P}(D)$ is called a field if and only if $\emptyset \in \mathcal{F}$, $D \in \mathcal{F}$ and for all A and B in $\mathcal{F}$, we have $A \cup B \in \mathcal{F}$ and $B \setminus A \in \mathcal{F}$. A field generated by a set of subsets C of D, denoted by $F(C)$, is the smallest field containing C, that is, the intersection of all fields containing C.*

Definition A.4 (Sigma field (σ-field)). *A field $\mathcal{F}$ with regard to a set D is called a σ-field if for any sequence ω of sets in $\mathcal{F}$ we have $\bigcup_{i=1}^{\#\omega} \omega[i] \in \mathcal{F}$.*

A σ-field generated by a set C of subsets of D is denoted by $\sigma(C)$.

Definition A.5 (Measurable space). *Let D be a non-empty set, and $\mathcal{F}$ a σ-field over D. Then $(D, \mathcal{F})$ is called a measurable space, and the sets in $\mathcal{F}$ are called measurable sets.*

Definition A.6 (Measure). *Let D be a non-empty set and $\mathcal{F}$ be a σ-field over D. A measure μ on $\mathcal{F}$ is a function that assigns a non-negative real value (possibly ∞) to each element of $\mathcal{F}$ such that*

1. $\mu(\emptyset) = 0$

2. *μ is σ-additive*

The measure μ is finite if $\mu(D) < \infty$. It is σ-finite if and only if D can be written as $\bigcup_{i=1}^{\#\phi} \phi[i]$, where $\phi[i] \in \mathcal{F}$ and $\mu(\phi[i]) < \infty$ for all i.

Definition A.7 (Probability measure). *Let D be a non-empty set and $\mathcal{F}$ be a σ-field over D. A probability measure μ is a measure on $\mathcal{F}$ such that*

$$\mu(D) = 1$$

Definition A.8 (Measure space). *A measure space is a triple $(D, \mathcal{F}, f)$, where $(D, \mathcal{F})$ is a measurable space, and f is a measure on $(D, \mathcal{F})$.*

Definition A.9 (Probability space). *A probability space is a triple $(D, \mathcal{F}, f)$ where $(D, \mathcal{F})$ is a measurable space, and f is a probability measure on $\mathcal{F}$.*

Definition A.10 (Measurable rectangle). *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be σ-fields over D_1 and D_2. Let D be the cartesian product of D_1 and D_2; $D_1 \times D_2$. A measurable rectangle in D is a set $A = A_1 \times A_2$, such that $A_1 \in \mathcal{F}_1$ and $A_2 \in \mathcal{F}_2$. The smallest σ-field containing all measurable rectangles of D is called the product σ-field, denoted by $\mathcal{F}_1 \overline{\times} \mathcal{F}_2$*[7].

Definition A.11 (Extensions of a set). *Let C be a set of subsets of a non-empty set D. We define a stepwise extension of C as follows:*

1. $F_1(C) \stackrel{\mathsf{def}}{=} C \cup \{\emptyset\} \cup \{D \setminus A \mid A \in C\}$

2. $F_2(C) \stackrel{\mathsf{def}}{=} \{\bigcap_{i=1}^{n} A_i \mid \forall i \in [1..n] : A_i \in F_1(C)\}$

3. $F_3(C) \stackrel{\mathsf{def}}{=} \{\bigcup_{i=1}^{n} A_i \mid \forall i \in [1..n] : A_i \in F_2(C) \wedge$
$\forall j, m \in [1..n] : j \neq m \Rightarrow A_j \cap A_m = \emptyset\}$

[7] The product σ-field of $\mathcal{F}_1$ and $\mathcal{F}_2$ is commonly denoted by $\mathcal{F}_1 \times \mathcal{F}_2$, but we use $\mathcal{F}_1 \overline{\times} \mathcal{F}_2$ to avoid confusion with the cross product of $\mathcal{F}_1$ and $\mathcal{F}_2$

B. Proofs

In this section we state all the lemmas and theorems and provide proofs for the ones that are not directly based on other sources. All proofs are written in Lamport's style for writing proofs [27]. This is a style for structuring formal proofs in a hierarchical manner in LaTeX [26], similar to that of natural deduction [51, 35]. As observed by Lamport the systematic structuring of proofs is essential to getting the results right in complex domains which it is difficult to have good intuitions about. We have had several iterations of formulating operators for component composition, attempting to prove them correct and then reformulating them when the structured proof style uncovered inconsistencies. These iterations where repeated until the definitions where proven to be correct.

The following tables give the page number for each theorem, lemma and corollary. If a theorem, lemma or corollary is used in proofs of other results we also include references to the results using it.

Result	Page	Used in proof of
Proposition B.1	Page 39	T 5.7
Lemma B.2	Page 41	T 5.7
Theorem B.3	Page 41	T 5.7,C 5.8
Theorem B.4	Page 41	L B.27

Table 1: List of results in Section B.1

Result	Page	Used in proof of
Lemma B.5	Page 41	C B.6
Corollary B.6	Page 41	L B.14
Corollary B.7	Page 42	L B.29
Lemma B.8	Page 42	L 5.6,L B.34,C 5.8
Lemma B.9	Page 42	C B.10,L B.11,L B.12
Corollary B.10	Page 43	L B.26,L B.35,L B.36
Lemma B.11	Page 43	L B.12,C B.13
Lemma B.12	Page 45	C B.13
Corollary B.13	Page 47	L B.14,C B.29
Lemma B.14	Page 47	C B.29,L B.38

Table 2: List of results in Section B.2

B.1. Measure theory

In the following we present some basic results from measure theory that we use in the later proofs. These are taken from other sources [9, 14, 24, 31, 1], and the proofs can be found there.

Proposition B.1. *Let C be a set of subsets of a non-empty set D and extend C to a set $F_3(C)$ as defined in Definition A.11. Then $C \subseteq FOCUS_1(C) \subseteq F_2(C) \subseteq F_3(C)$ and $F(C) = F_3(C)$, that is $F_3(C)$ is the field generated by C.*

Result	Page	Used in proof of
Lemma B.15	Page 49	L B.16
Lemma B.16	Page 49	L 5.5
Lemma B.17	Page 49	C B.18
Corollary B.18	Page 50	L B.26,L B.35,L B.36
Observation B.19	Page 50	L 5.4
Lemma B.20	Page 52	L 5.4
Lemma 5.4	Page 53	L B.26
Lemma B.21	Page 60	L B.24,L B.26
Lemma B.22	Page 60	L B.28,L B.23
Lemma B.23	Page 64	L B.24
Lemma B.24	Page 67	L B.26
Lemma B.25	Page 69	L B.26, L 5.6,L 5.6
Lemma B.26	Page 70	T 5.5
Theorem 5.5	Page 72	L B.28,L 5.6
Lemma B.27	Page 72	L B.28
Lemma B.28	Page 73	L 5.6,L B.29
Lemma 5.6	Page 77	T 5.7,C 5.8,L B.29
Lemma B.29	Page 78	L B.32,T 5.7
Lemma B.30	Page 82	C B.31
Corollary B.31	Page 83	L B.32
Lemma B.32	Page 84	L B.33,T 5.7
Lemma B.33	Page 89	T 5.7
Theorem 5.7	Page 90	C 5.8
Lemma B.34	Page 91	C 5.8,L B.39
Corollary 5.8	Page 92	T 5.9
Theorem 5.9	Page 93	

Table 3: List of results in Section B.3

Result	Page	Used in proof of
Lemma B.35	Page 93	C B.37
Lemma B.36	Page 95	C B.37
Corollary B.37	Page 97	L B.38
Lemma B.38	Page 97	L 7.2
Lemma 7.2	Page 102	T 7.6
Theorem 7.4	Page 102	T 7.6
Theorem 7.6	Page 102	

Table 4: List of results in Section B.4.

Lemma B.2. *Let C be a set of subsets of a non-empty set D. Then $\sigma(C) = \sigma(F(C))$.*

Theorem B.3 (Extension theorem). *A finite measure μ on a field F has a unique extension to the σ-field generated by F. That is, there exists a unique measure μ' on $\sigma(F)$ such that for each element C of F, $\mu'(C) = \mu(C)$.*

Theorem B.4 (Product Measure Theorem). *Let $(D_1, \mathcal{F}_1, \mu_1)$ and $(D_1, \mathcal{F}_1, \mu_1)$ be two measure spaces where μ_1 and μ_2 are σ-finite. Let $D = D_1 \times D_2$ and $\mathcal{F} = \mathcal{F}_1 \times \mathcal{F}_2$. Then there is a unique measure μ on $\mathcal{F}$, such that*

$$\mu(A_1 \times A_2) = \mu_1(A_1) \cdot \mu_2(A_2)$$

for every measurable rectangle $A_1 \times A_2 \in \mathcal{F}$. The measure μ is called the product of μ_1, μ_2 and the triplet $(D, \mathcal{F}, \mu)$ is called the product measure space.

B.2. Probabilistic component execution

In the following we state and prove some lemmas that we use to prove the main result in Section B.3; namely that we can construct a conditional probability measure on the cone-σ-field generated by the cone set obtained from the parallel execution of the trace sets of two probabilistic component executions.

Lemma B.5. ***(Adapted from Lemma 4.2.4 in Segala [43, p. 54]).*** *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

(1) $\forall t_1, t_2 \in D_N(\alpha) \colon t_1 \sqsubseteq t_2 \Rightarrow c(t_2, D_N(\alpha)) \subseteq c(t_1, D_N(\alpha))$

(2) $\forall t_1, t_2 \in D_N(\alpha) \colon t_1 \not\sqsubseteq t_2 \wedge t_2 \not\sqsubseteq t_1 \Rightarrow c(t_2, D_N(\alpha)) \cap c(t_1, D_N(\alpha)) = \emptyset$

Proof. Follows from Definition 3.1. □

Corollary B.6. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall c_1, c_2 \in C_E(D_N(\alpha)) \colon c_1 \cap c_2 \neq \emptyset \Rightarrow c_1 \subseteq c_2 \vee c_2 \subseteq c_1$$

Proof:

$\langle 1 \rangle 1.$ Assume: $c_1 \in C_E(D_N(\alpha)) \wedge c_2 \in C_E(D_N(\alpha))$
 Prove: $c_1 \cap c_2 \neq \emptyset \Rightarrow c_1 \subseteq c_2 \vee c_2 \subseteq c_1$
 $\langle 2 \rangle 1.$ Assume: $c_1 \cap c_2 \neq \emptyset$
  Prove: $c_1 \subseteq c_2 \vee c_2 \subseteq c_1$
  $\langle 3 \rangle 1.$ Case: $c_1 \in C_E(D_N(\alpha)) \setminus C(D_N(\alpha)) \vee c_2 \in C_E(D_N(\alpha)) \setminus C(D_N(\alpha))$
   $\langle 4 \rangle 1.$ Q.E.D.
    Proof: By assumption $\langle 3 \rangle 1$ and Definition 3.3 it follows that at least one of c_1 or c_2 contains only one trace. Since it is also the case, by assumption $\langle 2 \rangle 1$, that c_1 and c_2 shares at least one element, the required result follows from elementary set theory.
  $\langle 3 \rangle 2.$ Case: $c_1 \in C(D_N(\alpha)) \wedge c_2 \in C(D_N(\alpha))$
   $\langle 4 \rangle 1.$ $\exists t_1 \in \mathcal{H} \colon \exists t_2 \in \mathcal{H} \colon c_1 = c(t_1, D_N(\alpha)) \wedge c_2 = c(t_2, D_N(\alpha))$

PROOF: By assumption $\langle 3\rangle 2$ and Definition 3.1.

$\langle 4\rangle 2$. LET: $t_1 \in \mathcal{H}, t_2 \in \mathcal{H}$ such that $c_1 = c(t_1, D_N(\alpha)) \wedge c_2 = c(t_2, D_N(\alpha))$

PROOF: By $\langle 4\rangle 1$.

$\langle 4\rangle 3$. $c(t_1, D_N(\alpha)) \subseteq c(t_2, D_N(\alpha)) \vee c(t_2, D_N(\alpha)) \subseteq c(t_1, D_N(\alpha))$

$\langle 5\rangle 1$. $t_1 \sqsubseteq t_2 \vee t_2 \sqsubseteq t_1$

PROOF: By assumption $\langle 2\rangle 1$, $\langle 4\rangle 2$ and Lemma B.5 (2).

$\langle 5\rangle 2$. CASE: $t_2 \sqsubseteq t_1$

$\langle 6\rangle 1$. Q.E.D.

PROOF: By assumption $\langle 5\rangle 2$ and Lemma B.5 (1) $(c(t_1, D_N(\alpha)) \subseteq c(t_2, D_N(\alpha)))$ and $\vee$-introduction.

$\langle 5\rangle 3$. CASE: $t_1 \sqsubseteq t_2$

$\langle 6\rangle 1$. Q.E.D.

PROOF: By assumption $\langle 5\rangle 3$ and Lemma B.5 (1) $(c(t_2, D_N(\alpha)) \subseteq c(t_1, D_N(\alpha)))$ and $\vee$-introduction.

$\langle 5\rangle 4$. Q.E.D.

PROOF: By $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ and $\vee$ elimination.

$\langle 4\rangle 4$. Q.E.D.

PROOF: By $\langle 4\rangle 2$, $\langle 4\rangle 3$ and the rule of replacement [51].

$\langle 3\rangle 3$. Q.E.D.

PROOF: By assumption $\langle 1\rangle 1$, the cases $\langle 3\rangle 1$ and $\langle 3\rangle 2$ are exhaustive.

$\langle 2\rangle 2$. Q.E.D.

PROOF: $\Rightarrow$-introduction.

$\langle 1\rangle 2$. Q.E.D.

PROOF: $\forall$-introduction.

Corollary B.7. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then any union of elements in $C_E(D_N(\alpha))$ can be described as a disjoint union of elements in $C_E(D_N(\alpha))$.*

PROOF. Follows from Corollary B.6.

Lemma B.8. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall A, B \in \mathcal{F}_N(\alpha) : A \subseteq B \Rightarrow f_N(\alpha)(A) \leq f_N(\alpha)(B)$$

PROOF. Since $A \subseteq B$ we have $B = A \cup (B \cap (D_N(\alpha) \setminus A))$ where A and $B \cap (D_N(\alpha) \setminus A)$ are disjoint. Therefore $f_N(\alpha)(B) = f_N(\alpha)(A) + f_N(\alpha)(B \cap (D_N(\alpha) \setminus A)) \geq f_N(\alpha)(A)$.

Lemma B.9. *Let I_N be a probabilistic component execution as defined in Definition 5.3, let α be a complete queue history $\alpha \in \mathcal{B}_N$, and let S be a non-empty set of finite prefixes of traces in $D_N(\alpha)$. Then*

$$\bigcup_{t \in S} c(t, D_N(\alpha)) \text{ is a countable union of elements in } C(D_N(\alpha))$$

PROOF:

$\langle 1\rangle 1$. ASSUME: $S \neq \emptyset \wedge \forall t \in S : \exists t' \in D_N(\alpha) : t \sqsubseteq t' \wedge \#t \in \mathbb{N}$

PROVE: $\bigcup_{t \in S} c(t, D_N(\alpha))$ is a countable union of elements in $C(D_N(\alpha))$.

$\langle 2\rangle 1.$ $\forall t \in S : c(t, D_N(\alpha)) \in C(D_N(\alpha))$

PROOF: By assumption $\langle 1\rangle 1$ and Definition 3.3.

$\langle 2\rangle 2.$ $(\#S = \aleph_0 \vee \#S \in \mathbb{N})$, that is, S is countable.

$\langle 3\rangle 1.$ $\forall t \in S : \#t \in \mathbb{N}$

PROOF: By assumption $\langle 1\rangle 1$.

$\langle 3\rangle 2.$ Q.E.D.

PROOF: By $\langle 3\rangle 1$, since time-stamps are rational numbers and we assume that interfaces are assigned a countable number of signals, we have a countable number of events, and the set of finite sequences formed from a countable set is countable [25].

$\langle 2\rangle 3.$ Q.E.D.

PROOF: By $\langle 2\rangle 1$ and $\langle 2\rangle 2$.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$-introduction.

Corollary B.10. *Let I_N be a probabilistic component execution as defined in Definition 5.3, let α be a complete queue history $\alpha \in \mathcal{B}_N$, and let S be a (possibly empty) set of finite prefixes of traces in $D_N(\alpha)$. Then*

$$\bigcup_{t \in S} c(t, D_N(\alpha)) \in \mathcal{F}_N(\alpha)$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $\forall t \in S : \exists t' \in D_N(\alpha) : t \sqsubseteq t' \wedge \#t \in \mathbb{N}$

PROVE: $\bigcup_{t \in S} c(t, D_N(\alpha)) \in \mathcal{F}_N(\alpha)$.

$\langle 2\rangle 1.$ CASE: $S = \emptyset$

$\langle 3\rangle 1.$ Q.E.D.

PROOF: By Definition 5.2 and Definition 5.3.

$\langle 2\rangle 2.$ CASE: $S \neq \emptyset$

$\langle 3\rangle 1.$ $\forall t \in S : c(t, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)$

$\langle 4\rangle 1.$ $\forall t \in S : c(t, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)) \in C_E(D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha))$

PROOF: By assumption $\langle 1\rangle 1$ and Definition 3.3.

$\langle 4\rangle 2.$ Q.E.D.

PROOF: By $\langle 4\rangle 1$ since $C_E(D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)) \subseteq \mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)$

$\langle 3\rangle 2.$ $\bigcup_{t \in S} c(t, D_N(\alpha))$ is a countable union of elements.

PROOF: By assumption $\langle 1\rangle 1$, assumption $\langle 2\rangle 2$ and Lemma B.9.

$\langle 3\rangle 3.$ Q.E.D.

PROOF: By $\langle 3\rangle 1$ and $\langle 3\rangle 2$ since $\mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)$ is closed under countable union.

$\langle 2\rangle 3.$ Q.E.D.

PROOF: The cases $\langle 2\rangle 1$ and $\langle 2\rangle 2$ are exhaustive.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$-introduction.

Lemma B.11. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall t_1 \in (\mathcal{H} \cap \mathcal{E}^*) : c(t_1, D_N(\alpha)) \in C(D_N(\alpha)) \Rightarrow$$
$$D_N(\alpha) \setminus c(t_1, D_N(\alpha)) \textit{ is a countable union of elements in } C_E(D_N(\alpha)).$$

Proof:

$\langle 1\rangle 1.$ Assume: $t_1 \in (\mathcal{H} \cap \mathcal{E}^*)$

Prove: $c(t_1, D_N(\alpha)) \in C(D_N(\alpha)) \Rightarrow$
$D_N(\alpha) \setminus c(t_1, D_N(\alpha))$ is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 2\rangle 1.$ Assume: $c(t_1, D_N(\alpha)) \in C(D_N(\alpha))$

Prove: $D_N(\alpha) \setminus c(t_1, D_N(\alpha))$ is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 3\rangle 1.$ Let: $S = \{t \in \mathcal{H} | \exists t_2 \in D_N(\alpha) : t \sqsubseteq t_2 \wedge \#t \leq \#t_1 \wedge t \neq t_1\}$

$\langle 3\rangle 2.$ Case: $S = \emptyset$

$\langle 4\rangle 1.$ $D_N(\alpha) \setminus c(t_1, D_N(\alpha)) = \emptyset$

$\langle 5\rangle 1.$ Assume: $D_N(\alpha) \setminus c(t_1, D_N(\alpha)) \neq \emptyset$

Prove: $\perp$

$\langle 6\rangle 1.$ $\exists t \in D_N(\alpha) : t \notin c(t_1, D_N(\alpha))$

Proof: By assumption $\langle 5\rangle 1$.

$\langle 6\rangle 2.$ Let: $t \in D_N(\alpha)$ such that $t \notin c(t_1, D_N(\alpha))$

Proof: By $\langle 6\rangle 1$.

$\langle 6\rangle 3.$ $t_1 \not\sqsubseteq t$

Proof: By $\langle 6\rangle 2$ and Definition 3.1.

$\langle 6\rangle 4.$ $\exists t' \in \mathcal{H} : t' \sqsubseteq t \wedge \#t' \leq \#t_1 \wedge t' \neq t_1$

Proof: By $\langle 6\rangle 3$ and definition (2).

$\langle 6\rangle 5.$ Let: $t' \in \mathcal{H}$ such that $t' \sqsubseteq t \wedge \#t' \leq \#t_1 \wedge t' \neq t_1$

Proof: By $\langle 6\rangle 4$.

$\langle 6\rangle 6.$ $t' \in S$

Proof: By $\langle 3\rangle 1$, $\langle 6\rangle 2$ and $\langle 6\rangle 5$.

$\langle 6\rangle 7.$ $S \neq \emptyset$

Proof: By $\langle 6\rangle 5$ and $\langle 6\rangle 6$.

$\langle 6\rangle 8.$ Q.E.D.

Proof: By assumption $\langle 3\rangle 2$, $\langle 6\rangle 7$ and $\perp$ introduction.

$\langle 5\rangle 2.$ Q.E.D.

Proof: Proof by contradiction.

$\langle 4\rangle 2.$ $D_N(\alpha) = c(t_1, D_N(\alpha))$

Proof: By $\langle 4\rangle 1$ and elementary set theory.

$\langle 4\rangle 3.$ Q.E.D.

Proof: By assumption $\langle 2\rangle 1$, $\langle 4\rangle 2$ and the rule of replacement [51].

$\langle 3\rangle 3.$ Case: $S \neq \emptyset$

$\langle 4\rangle 1.$ $D_N(\alpha) \setminus c(t_1, D_N(\alpha)) = \bigcup_{t \in S} c(t, D_N(\alpha))$

$\langle 5\rangle 1.$ $\bigcup_{t \in S} c(t, D_N(\alpha)) \subseteq D_N(\alpha) \setminus c(t_1, D_N(\alpha))$

$\langle 6\rangle 1.$ Assume: $t_2 \in \bigcup_{t \in S} c(t, D_N(\alpha))$

Prove: $t_2 \in D_N(\alpha) \setminus c(t_1, D_N(\alpha))$

$\langle 7\rangle 1.$ $t_2 \in D_N(\alpha) \wedge t_2 \notin c(t_1, D_N(\alpha))$

$\langle 8\rangle 1.$ $t_2 \in D_N(\alpha)$

Proof: By assumption $\langle 6\rangle 1$, $\langle 3\rangle 1$ and Definition 3.1.

$\langle 8\rangle 2.$ $t_2 \notin c(t_1, D_N(\alpha))$

$\langle 9\rangle 1.$ $t_1 \not\sqsubseteq t_2$

$\langle 10\rangle 1.$ $\exists t \in \mathcal{H} : t \sqsubseteq t_2 \wedge \#t \leq \#t_1 \wedge t \neq t_2$

Proof: By assumption $\langle 6\rangle 1$ and $\langle 3\rangle 1$.

$\langle 10\rangle 2.$ Q.E.D.

Proof: By $\langle 10\rangle 1$ and definition (2).

$\langle 9\rangle 2$. Q.E.D.

PROOF: By $\langle 9\rangle 1$ and Definition 3.1.

$\langle 8\rangle 3$. Q.E.D.

PROOF: By $\langle 8\rangle 1$ and $\langle 8\rangle 2$ and $\wedge$-introduction.

$\langle 7\rangle 2$. Q.E.D.

PROOF: By $\langle 7\rangle 1$ and elementary set theory.

$\langle 6\rangle 2$. Q.E.D.

PROOF: By $\langle 6\rangle 1$ and $\subseteq$-rule [29]

$\langle 5\rangle 2$. $D_N(\alpha) \setminus c(t_1, D_N(\alpha)) \subseteq \bigcup_{t\in S} c(t, D_N(\alpha))$

$\langle 6\rangle 1$. ASSUME: $\exists t_2 \in \mathcal{H} : \in D_N(\alpha) \setminus c(t_1, D_N(\alpha)) \wedge t_2 \notin \bigcup_{t\in S} c(t, D_N(\alpha))$

PROVE: $\perp$

$\langle 7\rangle 1$. LET: t_2 be a trace such that $t_2 \in D_N(\alpha) \setminus c(t_1, D_N(\alpha)) \wedge$
$t_2 \notin \bigcup_{t\in S} c(t, D_N(\alpha))$

PROOF: By $\langle 6\rangle 1$.

$\langle 7\rangle 2$. $t_1 \not\sqsubseteq t_2$

PROOF: By Definition 3.1 and the first conjunct of $\langle 7\rangle 1$ which implies $t_2 \notin c(t_1, D_N(\alpha))$

$\langle 7\rangle 3$. $\exists t \in \mathcal{H} : \#t \leq \#t_1 \wedge t \sqsubseteq t_2 \wedge t \neq t_1$

PROOF: By $\langle 7\rangle 2$ and definition (2).

$\langle 7\rangle 4$. $t_2 \in \bigcup_{t\in S} c(t, D_N(\alpha))$

PROOF: By $\langle 7\rangle 3$ and $\langle 3\rangle 1$.

$\langle 7\rangle 5$. Q.E.D.

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 4$ and $\perp$-introduction.

$\langle 6\rangle 2$. Q.E.D.

PROOF: Proof by contradiction.

$\langle 5\rangle 3$. Q.E.D.

PROOF:By $\langle 5\rangle 1$, $\langle 5\rangle 2$ and =-rule for sets [29].

$\langle 4\rangle 2$. $\bigcup_{t\in S} c(t, D_N(\alpha))$ is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 5\rangle 1$. $\bigcup_{t\in S} c(t, D_N(\alpha))$ is a countable union of elements in $C(D_N(\alpha))$

PROOF: By assumption $\langle 1\rangle 1$, $\langle 3\rangle 1$, assumption $\langle 3\rangle 3$ and Lemma B.9.

$\langle 5\rangle 2$. Q.E.D.

PROOF: By $\langle 5\rangle 1$, since $C(D_N(\alpha)) \subseteq C_E(D_N(\alpha))$.

$\langle 4\rangle 3$. Q.E.D.

PROOF: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and the rule of replacement [51].

$\langle 3\rangle 4$. Q.E.D.

PROOF: The cases $\langle 3\rangle 2$ and $\langle 3\rangle 3$ are exhaustive.

$\langle 2\rangle 2$. Q.E.D.

PROOF: By $\Rightarrow$-introduction

$\langle 1\rangle 2$. Q.E.D.

PROOF: By $\forall$-introduction

Lemma B.12. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall t_1 \in (\mathcal{H} \cap \mathcal{E}^*) : \{t_1\} \in C_E(D_N(\alpha)) \setminus C(D_N(\alpha)) \Rightarrow$$
$$D_N(\alpha) \setminus \{t_1\} \textit{ is a countable union of elements in } C_E(D_N(\alpha))$$

PROOF:

$\langle 1 \rangle 1.$ Assume: $t_1 \in (\mathcal{H} \cap \mathcal{E}^*)$
Prove: $\{t_1\} \in C_E(D_N(\alpha)) \setminus C(D_N(\alpha)) \Rightarrow$
$D_N(\alpha) \setminus \{t_1\}$ is a countable union of elements in $C_E(D_N(\alpha))$

$\langle 2 \rangle 1.$ Assume: $\{t_1\} \in C_E(D_N(\alpha)) \setminus C(D_N(\alpha))$
Prove: $D_N(\alpha) \setminus \{t_1\}$ is a countable union of elements in $C_E(D_N(\alpha))$

$\langle 3 \rangle 1.$ $\#t_1 \in \mathbb{N}$
Proof: By assumption $\langle 2 \rangle 1$ and Definition 3.3.

$\langle 3 \rangle 2.$ $t_1 \in D_N(\alpha)$
Proof: By assumption $\langle 2 \rangle 1$ and Definition 3.3.

$\langle 3 \rangle 3.$ $D_N(\alpha) \setminus c(t_1, D_N(\alpha))$ is a countable union of elements in $C_E(D_N(\alpha))$.
Proof: By $\langle 3 \rangle 1$ and Lemma B.11.

$\langle 3 \rangle 4.$ Let: $S = \{t \in \mathcal{H} | \#t = \#t_1 + 1 \wedge \exists t' \in c(t_1, D_N(\alpha)) : t \sqsubseteq t'\}$

$\langle 3 \rangle 5.$ Case: $S = \emptyset$

$\langle 4 \rangle 1.$ $c(t_1, D_N(\alpha)) = \{t_1\}$
Proof: By $\langle 3 \rangle 4$ and assumption $\langle 3 \rangle 5$.

$\langle 4 \rangle 2.$ Q.E.D.
Proof: By $\langle 4 \rangle 1$, $\langle 3 \rangle 3$ and the rule of replacement [51].

$\langle 3 \rangle 6.$ Case: $S \neq \emptyset$

$\langle 4 \rangle 1.$ $(D_N(\alpha) \setminus c(t_1, D_N(\alpha))) \cup (\bigcup_{t \in S} c(t, D_N(\alpha)))$ is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 5 \rangle 1.$ $\bigcup_{t \in S} c(t, D_N(\alpha))$ is a countable union of elements in $C_E(D_N(\alpha))$

$\langle 6 \rangle 1.$ $\bigcup_{t \in S} c(t, D_N(\alpha))$ is a countable union of elements in $C(D_N(\alpha))$
Proof: By assumption $\langle 1 \rangle 1$, assumption $\langle 2 \rangle 1$, $\langle 3 \rangle 4$, assumption $\langle 3 \rangle 6$ and Lemma B.9.

$\langle 6 \rangle 2.$ Q.E.D.
Proof: By $\langle 6 \rangle 1$, since $C(D_N(\alpha)) \subseteq C_E(D_N(\alpha))$.

$\langle 5 \rangle 2.$ Q.E.D.
Proof: By $\langle 5 \rangle 1$, $\langle 3 \rangle 3$ and elementary set theory.

$\langle 4 \rangle 2.$ $D_N(\alpha) \setminus \{t_1\} = (D_N(\alpha) \setminus c(t_1, D_N(\alpha))) \cup (\bigcup_{t \in S} c(t, D_N(\alpha)))$

$\langle 5 \rangle 1.$ $c(t_1, D_N(\alpha)) \setminus \{t_1\} = \bigcup_{t \in S} c(t, D_N(\alpha))$

$\langle 6 \rangle 1.$ $c(t_1, D_N(\alpha)) \setminus \{t_1\} \subseteq \bigcup_{t \in S} c(t, D_N(\alpha))$

$\langle 7 \rangle 1.$ Assume: $t' \in c(t_1, D_N(\alpha)) \setminus \{t_1\}$
Prove: $t' \in \bigcup_{t \in S} c(t, D_N(\alpha))$

$\langle 8 \rangle 1.$ $t' \in D_N(\alpha)$
Proof: By assumption $\langle 7 \rangle 1$ and Definition 3.1.

$\langle 8 \rangle 2.$ $\exists t'' \in S : t'' \sqsubseteq t'$

$\langle 9 \rangle 1.$ $t' \in c(t_1, D_N(\alpha))$
Proof: By $\langle 7 \rangle 1$.

$\langle 9 \rangle 2.$ $t_1 \sqsubseteq t'$
Proof: By $\langle 9 \rangle 1$ and Definition 3.1.

$\langle 9 \rangle 3.$ $t_1 \neq t'$
Proof: By assumption $\langle 7 \rangle 1$.

$\langle 9 \rangle 4.$ $\#t' > \#t_1$
Proof: By $\langle 9 \rangle 2$ and $\langle 9 \rangle 3$.

$\langle 9 \rangle 5.$ $\exists t'' \in \mathcal{H} : \#t'' = \#t_1 + 1 \wedge t'' \sqsubseteq t'$
Proof: By $\langle 9 \rangle 4$, $\langle 9 \rangle 1$ and Definition 3.1.

$\langle 9 \rangle 6.$ Let: t'' be a trace such that $\#t'' = \#t_1 + 1 \wedge t'' \sqsubseteq t'$

PROOF: By $\langle 9\rangle 5$.

$\langle 9\rangle 7.$ $t'' \in S$

PROOF: By $\langle 3\rangle 4$, $\langle 9\rangle 6$ and $\langle 9\rangle 1$.

$\langle 9\rangle 8.$ Q.E.D.

PROOF: By $\langle 9\rangle 6$, $\langle 9\rangle 7$ and $\exists$-introduction.

$\langle 8\rangle 3.$ Q.E.D.

PROOF: By $\langle 8\rangle 1$, $\langle 8\rangle 2$ and Definition 3.1.

$\langle 7\rangle 2.$ Q.E.D.

PROOF: $\subseteq$-rule [29].

$\langle 6\rangle 2.$ $\bigcup_{t \in S} c(t, D_N(\alpha)) \subseteq c(t_1, D_N(\alpha)) \setminus \{t_1\}$

$\langle 7\rangle 1.$ $\bigcup_{t \in S} c(t, D_N(\alpha)) \subseteq c(t_1, D_N(\alpha))$

PROOF: By $\langle 3\rangle 4$, Lemma B.5 and elementary set theory.

$\langle 7\rangle 2.$ $t_1 \notin \bigcup_{t \in S} c(t, D_N(\alpha))$

PROOF: By $\langle 3\rangle 4$ and Definition 3.1.

$\langle 7\rangle 3.$ Q.E.D.

PROOF: By $\langle 7\rangle 1$ and $\langle 7\rangle 2$.

$\langle 6\rangle 3.$ Q.E.D.

PROOF: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and $=$-rule for sets [29].

$\langle 5\rangle 2.$ $D_N(\alpha) \setminus \{t_1\} = (D_N(\alpha) \setminus c(t_1, D_N(\alpha))) \cup (c(t_1, D_N(\alpha)) \setminus \{t_1\})$

$\langle 6\rangle 1.$ $\{t_1\} \subseteq c(t_1, D_N(\alpha))$

PROOF: By $\langle 3\rangle 2$ and Definition 3.1.

$\langle 6\rangle 2.$ $c(t_1, D_N(\alpha)) \subseteq D_N(\alpha)$

PROOF: By Definition 3.1.

$\langle 6\rangle 3.$ Q.E.D.

PROOF: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and elementary set theory.

$\langle 5\rangle 3.$ Q.E.D.

PROOF: By $\langle 5\rangle 1$, $\langle 5\rangle 2$ and the rule of transitivity [51].

$\langle 4\rangle 3.$ Q.E.D.

PROOF: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and the rule of replacement [51].

$\langle 3\rangle 7.$ Q.E.D.

PROOF: The cases $\langle 3\rangle 5$ and $\langle 3\rangle 6$ are exhaustive.

$\langle 2\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$-introduction

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\forall$-introduction

Corollary B.13. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall c \in C_E(D_N(\alpha)) : D_N(\alpha) \setminus c \textit{ is a countable union of elements in } C_E(D_N(\alpha)).$$

PROOF. Follows from Lemma B.11 and Lemma B.12.

Lemma B.14. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall A \in \mathcal{F}_N(\alpha) : A \textit{ is a countable union of elements in } C_E(D_N(\alpha)).$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $A \in \mathcal{F}_N(\alpha)$.
PROVE: A is a countable union of elements in $C_E(D_N(\alpha))$.

PROOF SKETCH:By induction on the construction of A.

$\langle 2\rangle 1.$ CASE: $A \in C_E(D_N(\alpha))$ (Induction basis)

$\langle 3\rangle 1.$ Q.E.D.

PROOF: By assumption $\langle 2\rangle 1$.

$\langle 2\rangle 2.$ CASE: $A = D_N(\alpha) \setminus B$ (induction step)

$\langle 3\rangle 1.$ ASSUME: B is a countable union of elements in $C_E(D_N(\alpha))$. (induction hypothesis)
PROVE: $D_N(\alpha) \setminus B$ is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 4\rangle 1.$ LET: ϕ be a sequence of elements in $C_E(D_N(\alpha))$ such that $B = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By $\langle 3\rangle 1$ and Definition A.1.

$\langle 4\rangle 2.$ $D_N(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i] = \bigcap_{i=1}^{\#\phi}(D_N(\alpha) \setminus \phi[i])$

PROOF: By the infinite version of De Morgan's laws (2.7) for sets [13].

$\langle 4\rangle 3.$ $\bigcap_{i=1}^{\#\phi}(D_N(\alpha) \setminus \phi[i])$ is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 5\rangle 1.$ $\forall i \in [1..\#\phi] : \bigcap_{i=1}^{\#\phi}(D_N(\alpha) \setminus \phi[i]) \subseteq (D_N(\alpha) \setminus \phi[i])$

PROOF: By elementary set theory [29].

$\langle 5\rangle 2.$ $\forall i \in [1..\#\phi] : D_N(\alpha) \setminus \phi[i]$ is a countable union of elements in $C_E(D_N(\alpha))$

PROOF: By $\langle 4\rangle 1$ and Corollary B.13.

$\langle 5\rangle 3.$ Q.E.D.

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$, since the subset of a countable set is countable.

$\langle 4\rangle 4.$ Q.E.D.

PROOF:By $\langle 4\rangle 2$, $\langle 4\rangle 3$ and the rule of replacement [51].

$\langle 3\rangle 2.$ Q.E.D.

PROOF: Induction step.

$\langle 2\rangle 3.$ CASE: A is a countable union of elements in $\mathcal{F}_N(\alpha)$

$\langle 3\rangle 1.$ ASSUME: All elements in A are countable unions of cones. (induction hypothesis)
PROVE: A is a countable union of elements in $C_E(D_N(\alpha))$.

$\langle 4\rangle 1.$ Q.E.D.

PROOF: By the induction hypothesis ($\langle 3\rangle 1$), since the union of countably many countable sets is countable [24].

$\langle 3\rangle 2.$ Q.E.D.

PROOF: Induction step.

$\langle 2\rangle 4.$ Q.E.D.

PROOF: By induction over the construction of A with $\langle 2\rangle 1$ as basis step and $\langle 2\rangle 2$ and $\langle 2\rangle 3$ as induction steps.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\forall$-introduction.

B.3. Conditional probability measure of a composite component

This subsection contains the proofs of all the theorems and lemmas in Section 5. We prove that our definition of a measure on a composite extended cone set (definition (25)) is well defined and σ-additive. We also show how this measure can be uniquely extended to a measure on the cone-σ-field generated by a composite extended cone set. The proof strategy for this result is inspired by Segala [43, p. 54-55], but the actual proofs differ from his since we have a different semantic model. Finally we show that our components are closed under composition.

Lemma B.15. ***(Adapted from Lemma 27 in Refsdal [37, p. 285]).*** *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Then*

$$\forall t \in D_N(\alpha) : \{t\} \in \mathcal{F}_N(\alpha)$$

Lemma B.16. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$, let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$ and let $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ be a measure on $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as defined in (25). Then*

$$\begin{aligned}\forall t_1 \in \mathcal{H} \cap \mathcal{E}^* : &\{t_1\} \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \setminus C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow\\ &(\mathcal{E}_{N_1} \circledS \{t_1\}) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \land (\mathcal{E}_{N_2} \circledS \{t_1\}) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)\end{aligned}$$

Proof:
Assume: $t_1 \in \mathcal{H} \cap \mathcal{E}^*$
Prove: $\{t_1\} \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \setminus C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$
$(\mathcal{E}_{N_1} \circledS \{t_1\}) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \land (\mathcal{E}_{N_2} \circledS \{t_1\}) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$
⟨2⟩1. Assume: $\{t_1\} \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \setminus C(D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $(\mathcal{E}_{N_1} \circledS \{t_1\}) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \land (\mathcal{E}_{N_2} \circledS \{t_1\}) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$
⟨3⟩1. $t_1 \in D_{N_1} \otimes D_{N_2}(\alpha)$
Proof: By assumption ⟨2⟩1 and Definition 3.3.
⟨3⟩2. $\mathcal{E}_{N_1} \circledS t_1 \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \land \mathcal{E}_{N_2} \circledS t_1 \in D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$
Proof: By ⟨3⟩1 and definition (22).
⟨3⟩3. Q.E.D.
Proof: By ⟨3⟩2 and Lemma B.15.
⟨2⟩2. Q.E.D.
Proof: $\Rightarrow$-introduction
⟨1⟩1. Q.E.D.
Proof: $\forall$-introduction.

Lemma B.17.

$$\begin{aligned}\forall t \in \mathcal{H} : \forall S \subseteq \mathcal{E} : \#(S \circledS t) \in \mathbb{N} \Rightarrow&\\ S \circledS t|_1 = S \circledS t \lor \exists i \in \mathbb{N} : S \circledS t|_i \neq S \circledS t \land S \circledS t|_{i+1} = S \circledS t&\end{aligned}$$

Proof:
⟨1⟩1. Assume: $t \in \mathcal{H} \land S \subseteq \mathcal{E}$
Prove: $\#(S \circledS t) \in \mathbb{N} \Rightarrow$
$S \circledS t|_1 = S \circledS t \lor \exists i \in \mathbb{N} : S \circledS t|_i \neq S \circledS t \land S \circledS t|_{i+1} = S \circledS t$
⟨2⟩1. Assume: $\#(S \circledS t) \in \mathbb{N}$
Prove: $S \circledS t|_1 = S \circledS t \lor \exists i \in \mathbb{N} : S \circledS t|_i \neq S \circledS t \land S \circledS t|_{i+1} = S \circledS t$
⟨3⟩1. Assume: $S \circledS t|_1 \neq S \circledS t \land \forall i \in \mathbb{N} : S \circledS t|_i \neq S \circledS t \Rightarrow S \circledS t|_{i+1} \neq S \circledS t$
Prove: $\perp$
⟨4⟩1. $S \circledS t \neq S \circledS t$

PROOF: By ⟨3⟩1 and the principle of mathematical induction.

⟨4⟩2. Q.E.D.

PROOF: By ⟨4⟩1 and $\perp$-introduction.

⟨3⟩2. Q.E.D.

PROOF: Proof by contradiction.

⟨2⟩2. Q.E.D.

PROOF: $\Rightarrow$-introduction.

⟨1⟩2. Q.E.D.

PROOF: $\forall$-introduction.

Corollary B.18.

$$\forall t \in \mathcal{H} : \forall S \subseteq \mathcal{E} : \#(S \circledS t) \in \mathbb{N} \Rightarrow \exists t' \in \mathcal{H} \cap \mathcal{E}^* : S \circledS t' = S \circledS t$$

PROOF. Follows from Lemma B.17.

Observation B.19. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$\begin{aligned}
&\forall t \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) :\\
&\quad ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha) \Rightarrow\\
&\qquad (\#t \in \mathbb{N} \Rightarrow \exists i \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t =\\
&\qquad\quad ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i) \wedge\\
&\qquad (\#t = \infty \Rightarrow \forall i \in \mathbb{N} : \exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge\\
&\qquad (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i)
\end{aligned}$$

PROOF:

⟨1⟩1. ASSUME: $t \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$
PROVE: $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha \Rightarrow$
$(\#t \in \mathbb{N} \Rightarrow \exists i \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i) \wedge$
$(\#t = \infty \Rightarrow \forall i \in \mathbb{N} : \exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i)$

⟨2⟩1. ASSUME: $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
PROVE: $(\#t \in \mathbb{N} \Rightarrow \exists i \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i) \wedge$
$(\#t = \infty \Rightarrow \forall i \in \mathbb{N} : \exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i)$

⟨3⟩1. $\#t \in \mathbb{N} \Rightarrow \exists i \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

⟨4⟩1. ASSUME: $\#t \in \mathbb{N}$
PROVE: $\exists i \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

$\langle 5\rangle 1.$ Q.E.D.

PROOF: By assumption $\langle 4\rangle 1$, assumption $\langle 2\rangle 1$ and definition (2).

$\langle 4\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$-introduction.

$\langle 3\rangle 2.$ $\#t = \infty \Rightarrow \forall i \in \mathbb{N} : \exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

$\langle 4\rangle 1.$ ASSUME: $\#t = \infty$
PROVE: $\forall i \in \mathbb{N} : \exists t' \in \mathcal{H} \cap {\mathcal{E}_{N_1}}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

$\langle 5\rangle 1.$ ASSUME: $i \in \mathbb{N}$
PROVE: $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

$\langle 6\rangle 1.$ ASSUME: $\forall t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \Rightarrow$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' \neq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$
PROVE: $\perp$

$\langle 7\rangle 1.$ $((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i \neq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

$\langle 8\rangle 1.$ $\exists j \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t|_j =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i$

$\langle 9\rangle 1.$ CASE: $i = 0$

$\langle 10\rangle 1.$ $(\{!\}\times\mathcal{S}\times N_1\times N_2\times\mathcal{Q}) \circledS t|_0 = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i$

PROOF: By assumption $\langle 9\rangle 1$.

$\langle 10\rangle 2.$ Q.E.D.

PROOF: By $\langle 10\rangle 1$ and $\exists$-introduction.

$\langle 9\rangle 2.$ CASE: $i \neq 0$

$\langle 10\rangle 1.$ $\exists j \in \mathbb{N} : t[j] =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i[\#\big(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i\big)]$

PROOF: By assumption $\langle 4\rangle 1$, assumption $\langle 9\rangle 2$ and definition (7).

$\langle 10\rangle 2.$ LET: $j \in \mathbb{N}$ such that $t[j] =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i[\#\big(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i\big)]$

PROOF: By $\langle 10\rangle 1$.

$\langle 10\rangle 3.$ $((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t|_j) = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i$

$\langle 11\rangle 1.$ $i = \#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t|_j)$

PROOF: By $\langle 10\rangle 2$

$\langle 11\rangle 2.$ Q.E.D.

PROOF: By $\langle 11\rangle 1$.

$\langle 10\rangle 4.$ Q.E.D.

PROOF: By $\langle 10\rangle 3$ and $\exists$-introduction.

$\langle 9\rangle 3.$ Q.E.D.

PROOF: The cases $\langle 9\rangle 1$ and $\langle 9\rangle 2$ are exhaustive.

$\langle 8\rangle 2.$ LET: $j \in \mathbb{N}$ such that $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t|_j =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i$

PROOF: By $\langle 8\rangle 1$.

⟨8⟩3. $t|_j \sqsubseteq t$

PROOF: By ⟨8⟩2, definition (2) and definition (3).

⟨8⟩4. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t|_j \neq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

PROOF: By assumption ⟨6⟩1, ⟨8⟩3 and $\forall$ elimination.

⟨8⟩5. Q.E.D.

PROOF: By ⟨8⟩2, ⟨8⟩4 and the rule of replacement [51].

⟨7⟩2. $((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t) \not\sqsubseteq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)$

PROOF: By assumption ⟨4⟩1, assumption ⟨5⟩1, ⟨7⟩1 and definition (2).

⟨7⟩3. Q.E.D.

PROOF: By assumption ⟨2⟩1, ⟨7⟩2 and $\perp$-introduction.

⟨6⟩2. Q.E.D.

PROOF: Proof by contradiction. Note that this holds even when $\#\alpha \in \mathbb{N}$, since by definition (3) $\alpha|_i = \alpha$ when $i > \#\alpha$.

⟨5⟩2. Q.E.D.

PROOF: $\forall$-introduction.

⟨4⟩2. Q.E.D.

PROOF: $\Rightarrow$-introduction

⟨3⟩3. Q.E.D.

PROOF: By ⟨3⟩1, ⟨3⟩2 and $\wedge$-introduction.

⟨2⟩2. Q.E.D.

PROOF: $\Rightarrow$-introduction.

⟨1⟩2. Q.E.D.

PROOF: $\forall$-introduction.

Lemma B.20. *Let s and t be two infinite sequences of events. Then*

$$s \neq t \Rightarrow \exists i \in \mathbb{N} : s|_i = t|_i \wedge s|_{i+1} \neq t|_{i+1}$$

PROOF:

⟨1⟩1. ASSUME: $s \neq t$
PROVE: $\exists i \in \mathbb{N} : s|_i = t|_i \wedge s|_{i+1} \neq t|_{i+1}$

⟨2⟩1. $s|_1 \neq t|_1 \vee (\exists i \in \mathbb{N} : s|_i = t|_i \wedge s|_{i+1} \neq t|_{i+1})$

⟨3⟩1. ASSUME: $s|_1 = t|_1 \wedge (\forall i \in \mathbb{N} : s|_i = t|_i \Rightarrow s|_{i+1} = t|_{i+1})$
PROVE: $\perp$

⟨4⟩1. $s = t$

PROOF: By ⟨3⟩1 and the principle of mathematical induction

⟨4⟩2. Q.E.D.

PROOF: By assumption ⟨1⟩1, ⟨4⟩1 and $\perp$-introduction.

⟨3⟩2. Q.E.D.

PROOF: Proof by contradiction.

⟨2⟩2. CASE: $s|_1 \neq t|_1$

⟨3⟩1. $s|_0 = t|_0$

PROOF: By assumption ⟨2⟩2, and the fact that $s|_0 = \langle\rangle \wedge t|_0 = \langle\rangle$.

⟨3⟩2. Q.E.D.

PROOF: By assumption ⟨2⟩2, ⟨3⟩1 and $\exists$ introduction, since we assume that $0 \in \mathbb{N}$.

⟨2⟩3. CASE: $\exists i \in \mathbb{N} : s|_i = t|_i \wedge s|_{i+1} \neq t|_{i+1}$

$\langle 3\rangle 1.$ Q.E.D.
PROOF: By assumption $\langle 2\rangle 3$.

$\langle 2\rangle 4.$ Q.E.D.
PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$ and $\vee$ elimination.

$\langle 1\rangle 2.$ Q.E.D.
PROOF: $\Rightarrow$-introduction.

Lemma 5.4 *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$CT_{N_1-N_2}(\alpha) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge CT_{N_2-N_1}(\alpha) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$$

PROOF:
$\langle 1\rangle 1.$ $CT_{N_1-N_2}(\alpha) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge CT_{N_2-N_1}(\alpha) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$
$\langle 2\rangle 1.$ $CT_{N_1-N_2}(\alpha) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
$\langle 3\rangle 1.$ CASE: $CT_{N_1-N_2}(\alpha) = \emptyset$
$\langle 4\rangle 1.$ Q.E.D.
PROOF: By assumption $\langle 3\rangle 1$, since $\emptyset \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ by Definition 5.2 and Definition 5.3.
$\langle 3\rangle 2.$ CASE: $CT_{N_1-N_2}(\alpha) \neq \emptyset$
$\langle 4\rangle 1.$ CASE: $\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha \in \mathbb{N}$
$\langle 5\rangle 1.$ LET: $S = \{t \in \mathcal{H}_{N_1} \cap \mathcal{E}^* \mid \exists t' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) : t \sqsubseteq t' \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t = (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha\}$
$\langle 5\rangle 2.$ LET: $S' = \{t \in \mathcal{H}_{N_1} \cap \mathcal{E}^* \mid \exists t' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) : t \sqsubseteq t' \wedge$
$\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t =$
$\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha) + 1\}$
$\langle 5\rangle 3.$ $\bigcup_{t \in S} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \setminus \bigcup_{t \in S'} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
$\langle 6\rangle 1.$ $\bigcup_{t \in S} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
PROOF: By, $\langle 5\rangle 1$ and Corollary B.10.
$\langle 6\rangle 2.$ $\bigcup_{t \in S'} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
PROOF: By, $\langle 5\rangle 2$ and Corollary B.10.
$\langle 6\rangle 3.$ Q.E.D.
PROOF: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$, since $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ is closed under set difference.
$\langle 5\rangle 4.$ $\bigcup_{t \in S} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \setminus \bigcup_{t \in S'} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) = CT_{N_1-N_2}(\alpha)$
$\langle 6\rangle 1.$ $\bigcup_{t \in S} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \setminus \bigcup_{t \in S'} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \subseteq CT_{N_1-N_2}(\alpha)$
$\langle 7\rangle 1.$ ASSUME: $t \in \bigcup_{t' \in S} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \setminus \bigcup_{t' \in S'} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$
PROVE: $t \in CT_{N_1-N_2}(\alpha)$
$\langle 8\rangle 1.$ $t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
PROOF: By assumption $\langle 7\rangle 1$, $\langle 5\rangle 1$ and Definition 3.1.
$\langle 8\rangle 2.$ $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
$\langle 9\rangle 1.$ $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
PROOF: By assumption $\langle 7\rangle 1$ and, which implies that $S \neq \emptyset$.
$\langle 9\rangle 2.$ LET: $t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^*$ such that $t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
PROOF: By $\langle 9\rangle 1$.

$\langle 9\rangle$3. $\neg\exists i \in [\#t'..\#t] : k.t[i] = ! \wedge tr.t[i] = N_1 \wedge co.t[i] = N_2$

$\langle 10\rangle$1. Assume: $\exists i \in [\#t'..\#t] : k.t[i] = ! \wedge tr.t[i] = N_1 \wedge co.t[i] = N_2$

Prove: $\perp$

$\langle 11\rangle$1. Let: $i \in [\#t'..\#t]$ such that
$k.t[i] = ! \wedge tr.t[i] = N_1 \wedge co.t[i] = N_2$

Proof: By $\langle 10\rangle$1.

$\langle 11\rangle$2. $\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t \geq$
$\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, \alpha + 1$

Proof: By $\langle 9\rangle$2 and $\langle 11\rangle$1.

$\langle 11\rangle$3. $\exists t'' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t'' \sqsubseteq t \wedge \#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t'' =$
$\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, \alpha + 1$

Proof: By assumption $\langle 4\rangle$1 and $\langle 11\rangle$2.

$\langle 11\rangle$4. Let: $t'' \in \mathcal{H}_{N_1} \cap \mathcal{E}^*$ such that
$t'' \sqsubseteq t \wedge \#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t'' =$
$\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, \alpha + 1$

Proof: By $\langle 11\rangle$3.

$\langle 11\rangle$5. $t'' \in S'$

Proof: By $\langle 11\rangle$4, $\langle 8\rangle$1 and $\langle 5\rangle$2.

$\langle 11\rangle$6. $t \in c(t'', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha))$

Proof: By $\langle 11\rangle$4, $\langle 8\rangle$1 and Definition 3.1.

$\langle 11\rangle$7. $t \in \bigcup_{t' \in S'} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha))$

Proof: By $\langle 11\rangle$5, $\langle 11\rangle$6 and elementary set theory.

$\langle 11\rangle$8. Q.E.D.

Proof: By assumption $\langle 7\rangle$1, $\langle 11\rangle$7 and $\perp$ introduction.

$\langle 10\rangle$2. Q.E.D.

Proof: Proof by contradiction.

$\langle 9\rangle$4. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t|_{\#t'} = (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t$

Proof: By $\langle 9\rangle$3 and definition (7).

$\langle 9\rangle$5. Q.E.D.

Proof: By $\langle 9\rangle$2, $\langle 9\rangle$4 and the rule of replacement [51].

$\langle 8\rangle$3. Q.E.D.

Proof: By $\langle 8\rangle$1, $\langle 8\rangle$2 and definition (24).

$\langle 7\rangle$2. Q.E.D.

Proof: $\subseteq$ rule.

$\langle 6\rangle$2. $CT_{N_1-N_2}(\alpha) \subseteq \bigcup_{t \in S} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha)) \setminus \bigcup_{t \in S'} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha))$

$\langle 7\rangle$1. Assume: $t \in CT_{N_1-N_2}(\alpha)$

Prove: $t \in \bigcup_{t' \in S} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha)) \setminus \bigcup_{t' \in S'} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha))$

$\langle 8\rangle$1. $t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha)$

Proof: By assumption $\langle 7\rangle$1 and definition (24).

$\langle 8\rangle$2. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, \alpha$

Proof: By assumption $\langle 7\rangle$1 and definition (24).

$\langle 8\rangle$3. $\exists i \in \mathbb{N} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t|_i =$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, \alpha$

Proof: By assumption $\langle 4\rangle$1, $\langle 8\rangle$2 and Corollary B.18.

$\langle 8\rangle$4. Let: $i \in \mathbb{N}$ such that $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, t|_i =$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS\, \alpha$

PROOF: By ⟨8⟩3.

⟨8⟩5. $t \in \bigcup_{t' \in S} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

⟨9⟩1. $t|_i \in S$

PROOF: By ⟨8⟩1, ⟨8⟩4 and ⟨5⟩1.

⟨9⟩2. $t \in c(t|_i, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

PROOF: By ⟨8⟩1 and Definition 3.1.

⟨9⟩3. Q.E.D.

PROOF: By ⟨9⟩2, ⟨9⟩1 and elementary set theory.

⟨8⟩6. $t \notin \bigcup_{t' \in S'} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

⟨9⟩1. ASSUME: $t \in \bigcup_{t' \in S'} c(t', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$
PROVE: $\perp$

⟨10⟩1. $\exists j \in [i+1..\#t] : k.t[j] = ! \wedge tr.t[j] = N_1 \wedge co.t[j] = N_2$

⟨11⟩1. $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge \#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha) + 1$

PROOF: By assumption ⟨9⟩1 and ⟨5⟩2.

⟨11⟩2. LET: $t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^*$ such that $t' \sqsubseteq t \wedge$
$\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha) + 1$

PROOF: By ⟨11⟩1.

⟨11⟩3. LET: $j = \#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t')$

⟨11⟩4. $j \in [i+1..\#t] \wedge k.t[j] = ! \wedge tr.t[j] = N_1 \wedge co.t[j] = N_2$

PROOF: By ⟨8⟩4, ⟨11⟩2 and ⟨11⟩3.

⟨11⟩5. Q.E.D.

PROOF: By ⟨11⟩3, ⟨11⟩4 and $\exists$ introduction.

⟨10⟩2. LET: $j \in [i+1..\#t]$ such that
$k.t[j] = ! \wedge tr.t[j] = N_1 \wedge co.t[j] = N_2$

PROOF: By ⟨10⟩1.

⟨10⟩3. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \not\sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

PROOF: By ⟨8⟩4, ⟨10⟩2 and definition (2).

⟨10⟩4. Q.E.D.

PROOF: By ⟨8⟩2, ⟨10⟩3 and $\perp$ introduction.

⟨9⟩2. Q.E.D.

PROOF: Proof by contradiction.

⟨8⟩7. Q.E.D.

PROOF: By ⟨8⟩5, ⟨8⟩6 and elementary set theory.

⟨7⟩2. Q.E.D.

PROOF: $\subseteq$ rule.

⟨6⟩3. Q.E.D.

PROOF: By ⟨6⟩1, ⟨6⟩2 and the =-rule for sets [29].

⟨5⟩5. Q.E.D.

PROOF: By ⟨5⟩3, ⟨5⟩4 and the rule of replacement [51].

⟨4⟩2. CASE: $\#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha = \infty$

⟨5⟩1. LET: $S = \{t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap \mathcal{E}^* \mid (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)\}$

⟨5⟩2. $\forall i \in \mathbb{N}$

Let: $S'_i = \big\{t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* \mid \exists t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i\big\}$

⟨5⟩3. $\forall i \in \mathbb{N}$
Let: $G_i = \bigcup_{t \in S'_i} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

⟨5⟩4. $S \cup \bigcap_{i=1}^{\infty} G_i \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

⟨6⟩1. $S \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

⟨7⟩1. $\forall t \in \bigcup_{t' \in S}\{t'\} : \{t\} \in \mathcal{F}$
Proof: By ⟨5⟩1 and Lemma B.15.

⟨7⟩2. $(\#S = \aleph_0 \vee \#S \in \mathbb{N})$, that is, S is countable.

⟨8⟩1. $\forall t \in S : \#t \in \mathbb{N}$
Proof: By ⟨5⟩1.

⟨8⟩2. Q.E.D.
Proof: By ⟨8⟩1, since the set of finite sequences formed from a countable set is countable [25].

⟨7⟩3. Q.E.D.
Proof: By ⟨7⟩1 and ⟨7⟩2, since $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ is closed under countable union.

⟨6⟩2. $\bigcap_{i=1}^{\infty} G_i \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

⟨7⟩1. $\forall i \in \mathbb{N} : G_i \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
Proof: By ⟨5⟩2 and Corollary B.10.

⟨7⟩2. Q.E.D.
Proof: By ⟨7⟩1, since $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ is closed under countable intersection.

⟨6⟩3. Q.E.D.
Proof: By ⟨6⟩1 and ⟨6⟩2, since $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ is closed under countable union.

⟨5⟩5. $S \cup \bigcap_{i=1}^{\infty} G_i = CT_{N_1 - N_2}(\alpha)$

⟨6⟩1. $S \cup \bigcap_{i=1}^{\infty} G_i \subseteq CT_{N_1 - N_2}(\alpha)$

⟨7⟩1. Assume: $t \in S \cup \bigcap_{i=1}^{\infty} G_i$
Prove: $t \in CT_{N_1 - N_2}(\alpha)$

⟨8⟩1. Case: $t \in S$

⟨9⟩1. Q.E.D.
Proof: By ⟨5⟩1 and definition (24).

⟨8⟩2. Case: $t \in \bigcap_{i=1}^{\infty} G_i$

⟨9⟩1. $\forall i \in \mathbb{N} : t \in G_i$
Proof: By assumption ⟨8⟩2.

⟨9⟩2. $\#t = \infty$

⟨10⟩1. Assume: $\#t \in \mathbb{N}$
Prove: $\perp$

⟨11⟩1. $t \in G_{\#t+1}$
Proof: By assumption ⟨10⟩1, ⟨9⟩1 and $\forall$ elimination.

⟨11⟩2. $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{\#t+1}$
Proof: By ⟨11⟩1, ⟨5⟩3 and ⟨5⟩2.

⟨11⟩3. Let: $t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$

$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{\#t+1}$

PROOF: By $\langle 11\rangle 2$.

$\langle 11\rangle 4$. $\#t' >= \#t + 1$

$\langle 12\rangle 1$. $\#t' >= \#(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t'$

PROOF: By definition (7).

$\langle 12\rangle 2$. $\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t') =$
$\#(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{\#t+1})$

PROOF: By $\langle 11\rangle 3$ and the rule of equality between functions [51].

$\langle 12\rangle 3$. $\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{\#t+1} = \#t + 1$

PROOF: By assumption $\langle 4\rangle 2$.

$\langle 12\rangle 4$. Q.E.D.

PROOF: By $\langle 12\rangle 2$, $\langle 12\rangle 3$, $\langle 12\rangle 1$ and the rule of transitivity [51].

$\langle 11\rangle 5$. $t' \not\sqsubseteq t$

PROOF: By $\langle 11\rangle 4$ and definition (2).

$\langle 11\rangle 6$. Q.E.D.

PROOF: By $\langle 11\rangle 3$, $\langle 11\rangle 5$ and $\bot$ introduction.

$\langle 10\rangle 2$. Q.E.D.

PROOF: Proof by contradiction.

$\langle 9\rangle 3$. ASSUME: $t \notin CT_{N_1-N_2}(\alpha)$
PROVE: $\bot$

$\langle 10\rangle 1$. $t \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$

PROOF: By assumption $\langle 8\rangle 2$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ and Definition 3.1.

$\langle 10\rangle 2$. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \not\sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

PROOF: By $\langle 10\rangle 1$, assumption $\langle 9\rangle 3$ and definition (24).

$\langle 10\rangle 3$. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \neq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

PROOF: By $\langle 10\rangle 2$ and definition (2).

$\langle 10\rangle 4$. $\exists i \in \mathbb{N} : ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i \wedge$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_{i+1} \neq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1}$

PROOF: By $\langle 9\rangle 2$, assumption $\langle 4\rangle 2$, $\langle 10\rangle 3$ and Lemma B.20.

$\langle 10\rangle 5$. LET: $i \in \mathbb{N}$ such that $((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_i =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i \wedge$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_{i+1} \neq$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1}$

PROOF: By $\langle 10\rangle 4$.

$\langle 10\rangle 6$. $t \in G_{i+1}$

PROOF: By $\langle 10\rangle 5$, $\langle 9\rangle 1$ and $\forall$ elimination.

$\langle 10\rangle 7$. $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1}$

PROOF: By $\langle 10\rangle 6$, $\langle 5\rangle 3$ and $\langle 5\rangle 2$.

$\langle 10\rangle 8$. LET: $t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1}$

Proof: By $\langle 10\rangle 7$.

$\langle 10\rangle 9.$ $((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_{i+1} = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1}$

$\langle 11\rangle 1.$ $((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_{i+1} =$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t'$

$\langle 12\rangle 1.$ $\#(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_{i+1}) =$
$\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t')$

$\langle 13\rangle 1.$ $\#(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t)|_{i+1}) = i + 1$

Proof: By $\langle 9\rangle 2$ and definition (2).

$\langle 13\rangle 2.$ $\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t') = i + 1$

$\langle 14\rangle 1.$ $\#((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t') =$
$\#(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1})$

Proof: By $\langle 10\rangle 8$ and the rule of equality between functions [51].

$\langle 14\rangle 2.$ $\#(((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_{i+1}) = i + 1$

Proof: By assumption $\langle 4\rangle 2$ and definition (2).

$\langle 14\rangle 3.$ Q.E.D.

Proof: By $\langle 14\rangle 1$, $\langle 14\rangle 2$ and the rule of transitivity.

$\langle 13\rangle 3.$ Q.E.D.

Proof: By $\langle 13\rangle 1$, $\langle 13\rangle 2$ and the rule of transitivity.

$\langle 12\rangle 2.$ Q.E.D.

Proof: By $\langle 10\rangle 8$ ($t' \sqsubseteq t$), $\langle 12\rangle 1$ definition (2) and definition (7).

$\langle 11\rangle 2.$ Q.E.D.

Proof: By $\langle 10\rangle 8$, $\langle 11\rangle 1$ and the rule of transitivity [51].

$\langle 10\rangle 10.$ Q.E.D.

Proof: By $\langle 10\rangle 5$, $\langle 10\rangle 9$ and $\perp$-introduction.

$\langle 9\rangle 4.$ Q.E.D.

Proof: Proof by contradiction.

$\langle 8\rangle 3.$ Q.E.D.

Proof: By assumption $\langle 7\rangle 1$, the cases $\langle 8\rangle 1$ and $\langle 8\rangle 2$ are exhaustive.

$\langle 7\rangle 2.$ Q.E.D.

Proof: $\subseteq$ rule.

$\langle 6\rangle 2.$ $CT_{N_1 - N_2}(\alpha) \subseteq S \cup \bigcap_{i=1}^{\infty} G_i$

$\langle 7\rangle 1.$ Assume: $t \in CT_{N_1 - N_2}(\alpha)$
Prove: $t \in S \cup \bigcap_{i=1}^{\infty} G_i$

$\langle 8\rangle 1.$ $t \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

Proof: By assumption $\langle 7\rangle 1$ and definition (24).

$\langle 8\rangle 2.$ Case: $\#t \in \mathbb{N}$

$\langle 9\rangle 1.$ $t \in S$

Proof: By $\langle 8\rangle 1$, assumption $\langle 8\rangle 2$ and $\langle 5\rangle 1$.

$\langle 9\rangle 2.$ Q.E.D.

Proof: By $\langle 9\rangle 1$ and elementary set theory.

$\langle 8\rangle 3.$ Case: $\#t = \infty$

$\langle 9\rangle 1.$ $t \in \bigcap_{i=1}^{\infty} G_i$

$\langle 10\rangle 1.$ Assume: $t \notin \bigcap_{i=1}^{\infty} G_i$
Prove: $\perp$

$\langle 11\rangle 1.$ $\exists i \in \mathbb{N} : t \notin G_i$

PROOF: By assumption $\langle 10\rangle 1$.

$\langle 11\rangle 2.$ LET: $i \in \mathbb{N}$ such that $t \notin G_i$

PROOF: By $\langle 11\rangle 1$.

$\langle 11\rangle 3.$ $\neg\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' = ((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

$\langle 12\rangle 1.$ ASSUME: $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

PROVE: $\perp$

$\langle 13\rangle 1.$ LET: $t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

PROOF: By $\langle 12\rangle 1$.

$\langle 13\rangle 2.$ $t' \in S'_i$

PROOF: By $\langle 8\rangle 1$, $\langle 13\rangle 1$ and $\langle 5\rangle 2$.

$\langle 13\rangle 3.$ $t \in G_i$

PROOF: By $\langle 8\rangle 1$, $\langle 13\rangle 1$, $\langle 13\rangle 2$, Definition 3.1 and $\langle 5\rangle 3$.

$\langle 13\rangle 4.$ Q.E.D.

PROOF: By $\langle 11\rangle 2$, $\langle 13\rangle 3$ and $\perp$ introduction.

$\langle 12\rangle 2.$ Q.E.D.

PROOF: Proof by contradiction.

$\langle 11\rangle 4.$ $\exists t' \in \mathcal{H}_{N_1} \cap \mathcal{E}^* : t' \sqsubseteq t \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t' =$
$((\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha)|_i$

PROOF: By $\langle 8\rangle 1$, assumption $\langle 8\rangle 3$, Observation B.19 and $\forall$ elimination.

$\langle 11\rangle 5.$ Q.E.D.

PROOF: By $\langle 11\rangle 3$, $\langle 11\rangle 4$ and $\perp$-introduction.

$\langle 10\rangle 2.$ Q.E.D.

PROOF: Proof by contradiction.

$\langle 9\rangle 2.$ Q.E.D.

PROOF: By $\langle 9\rangle 1$ and elementary set theory.

$\langle 8\rangle 4.$ Q.E.D.

PROOF: The cases $\langle 8\rangle 2$ and $\langle 8\rangle 3$ are exhaustive.

$\langle 7\rangle 2.$ Q.E.D.

PROOF: $\subseteq$ rule.

$\langle 6\rangle 3.$ Q.E.D.

PROOF: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and the $=$-rule for sets [29].

$\langle 5\rangle 6.$ Q.E.D.

PROOF: By $\langle 5\rangle 4$, $\langle 5\rangle 5$ and the rule of replacement [51].

$\langle 4\rangle 3.$ Q.E.D.

PROOF: The cases $\langle 4\rangle 1$ and $\langle 4\rangle 2$ are exhaustive.

$\langle 3\rangle 3.$ Q.E.D.

PROOF: The cases $\langle 3\rangle 1$ and $\langle 3\rangle 2$ are exhaustive.

$\langle 2\rangle 2.$ $CT_{N_2-N_1}(\alpha) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

PROOF: Symmetrical to $\langle 2\rangle 1$.

⟨2⟩3. Q.E.D.

PROOF: By ⟨2⟩1, ⟨2⟩2 and $\wedge$ -introduction.

⟨1⟩2. Q.E.D.

Lemma B.21. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$\forall t_1 \in \mathcal{H} \cap \mathcal{E}^* : c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$$
$$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha))$$

PROOF:

⟨1⟩1. ASSUME: $t_1 \in \mathcal{H} \cap \mathcal{E}^*$

PROVE: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$
$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$

⟨2⟩1. ASSUME: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))$

PROVE: $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$

⟨3⟩1. ASSUME: $t' \in \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

PROVE: $t' \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha))$

⟨4⟩1. $\exists t'' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t' = \mathcal{E}_{N_1} \circledS t''$

PROOF: By assumption ⟨3⟩1 and definition (7).

⟨4⟩2. LET: $t'' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$ such that $t' = \mathcal{E}_{N_1} \circledS t''$

PROOF: By ⟨4⟩1.

⟨4⟩3. $t' \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$

⟨5⟩1. $\mathcal{E}_{N_1} \circledS t'' \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)$

PROOF: By ⟨4⟩2, definition (22) and Definition 3.1.

⟨5⟩2. Q.E.D.

PROOF: By ⟨4⟩2, ⟨5⟩1 and the rule of replacement [51].

⟨4⟩4. $\mathcal{E}_{N_1} \circledS t_1 \sqsubseteq t'$

⟨5⟩1. $\mathcal{E}_{N_1} \circledS t_1 \sqsubseteq \mathcal{E}_{N_1} \circledS t''$

⟨6⟩1. $t_1 \sqsubseteq t''$

PROOF: By ⟨4⟩2 and Definition 3.1.

⟨6⟩2. Q.E.D.

PROOF: By ⟨6⟩1 and definition (7).

⟨5⟩2. Q.E.D.

PROOF: By ⟨5⟩1, ⟨4⟩2 and the rule of replacement [51].

⟨4⟩5. Q.E.D.

PROOF: By ⟨4⟩3, ⟨4⟩4 and Definition 3.1.

⟨3⟩2. Q.E.D.

PROOF: By ⟨3⟩1 and $\subseteq$-rule [29].

⟨2⟩2. Q.E.D.

PROOF: $\Rightarrow$-introduction.

⟨1⟩2. Q.E.D.

PROOF: $\forall$-introduction.

Lemma B.22. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that*

$N_1 \cap N_2 = \emptyset$ *and let* α *be a queue history in* $\mathcal{B}_{N_1 \cup N_2}$*. Then*

$$\begin{aligned}
&\forall t \in \mathcal{H} \cap \mathcal{E}^* : c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow \\
&(\forall t_1, t_2 \in \mathcal{H} : t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow \\
&\qquad\qquad (\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2)
\end{aligned}$$

Proof:

$\langle 1 \rangle 1.$ Assume: $t \in \mathcal{H} \cap \mathcal{E}^*$
Prove: $c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$
$(\forall t_1, t_2 \in \mathcal{H} : t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge$
$t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$
$(\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2)$

$\langle 2 \rangle 1.$ Assume: $c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $\forall t_1, t_2 \in \mathcal{H} : t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge$
$t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$
$(\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2)$

Proof sketch: By induction over the length of t.

$\langle 3 \rangle 1.$ Case: $t = \langle\rangle$ (induction basis)

$\langle 4 \rangle 1.$ Assume: $t_1 \in \mathcal{H} \wedge t_2 \in \mathcal{H}$
Prove: $t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$
$\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

$\langle 5 \rangle 1.$ Assume: $t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

$\langle 6 \rangle 1.$ $c(t, D_{N_1} \otimes D_{N_2}(\alpha)) = D_{N_1} \otimes D_{N_2}(\alpha)$
Proof: By assumption $\langle 3 \rangle 1$ and Definition 3.1.

$\langle 6 \rangle 2.$ $\exists t'', t''' \in D_{N_1} \otimes D_{N_2}(\alpha) : \mathcal{E}_{N_1} \circledS t'' = t_1 \wedge \mathcal{E}_{N_2} \circledS t''' = t_2$
Proof: By assumption $\langle 5 \rangle 1$, $\langle 6 \rangle 1$ and definition (7).

$\langle 6 \rangle 3.$ Let: $t'', t''' \in D_{N_1} \otimes D_{N_2}(\alpha)$ such that $\mathcal{E}_{N_1} \circledS t'' = t_1 \wedge \mathcal{E}_{N_2} \circledS t''' = t_2$
Proof: By $\langle 6 \rangle 2$

$\langle 6 \rangle 4.$ $t_1 \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge t_2 \in D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

$\langle 7 \rangle 1.$ $t_1 \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

$\langle 8 \rangle 1.$ $\mathcal{E}_{N_1} \circledS t'' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
Proof: By $\langle 6 \rangle 3$ and definition (22).

$\langle 8 \rangle 2.$ Q.E.D.
Proof: By $\langle 6 \rangle 3$, $\langle 8 \rangle 1$ and the rule of replacement [51].

$\langle 7 \rangle 2.$ $t_2 \in D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$
Proof: Symmetrical to $\langle 7 \rangle 1$.

$\langle 7 \rangle 3.$ Q.E.D.
Proof: By $\langle 7 \rangle 1$, $\langle 7 \rangle 2$ and $\wedge$-introduction.

$\langle 6 \rangle 5.$ $\mathsf{rng}.t_1 \subseteq \mathcal{E}_{N_1} \wedge \mathsf{rng}.t_2 \subseteq \mathcal{E}_{N_2}$
Proof: By $\langle 6 \rangle 4$, Definition 5.3, definition (20) and definition (5).

$\langle 6 \rangle 6.$ $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t_1 \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha \wedge$
$(\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS t_2 \sqsubseteq (\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS \alpha$

$\langle 7 \rangle 1.$ $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t_1 \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

$\langle 8 \rangle 1.$ $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t'' \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
Proof: By $\langle 6 \rangle 3$ and definition (22).

$\langle 8\rangle 2.$ $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \mathcal{E}_{N_1} \circledS t'' \sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

Proof: By $\langle 8\rangle 1$ and definition (7).

$\langle 8\rangle 3.$ Q.E.D.

Proof: By $\langle 6\rangle 3$, $\langle 8\rangle 2$ and the rule of replacement [51].

$\langle 7\rangle 2.$ $(\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS t_2 \sqsubseteq (\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS \alpha$

Proof: Symmetrical to step $\langle 7\rangle 1$

$\langle 7\rangle 3.$ Q.E.D.

Proof: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\wedge$ -introduction.

$\langle 6\rangle 7.$ $((\forall i, j \in [1..\#t_1] : i < j \Rightarrow q.t_1[i] < q.t_1[j]) \wedge$
$\#t_1 = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t_1[i] > k) \wedge$
$(\forall i, j \in [1..\#t_2] : i < j \Rightarrow q.t_2[i] < q.t_2[j] \wedge$
$\#t_2 = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t_2[i] > k)$

$\langle 7\rangle 1.$ $(\forall i, j \in [1..\#t_1] : i < j \Rightarrow q.t_1[i] < q.t_1[j]) \wedge$
$(\#t_1 = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t_1[i] > k)$

$\langle 8\rangle 1.$ $\forall i, j \in [1..\#t''] : i < j \Rightarrow q.t''[i] < q.t''[j] \wedge$
$\#t'' = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t''[i] > k$

Proof: By $\langle 6\rangle 3$ and definition (22).

$\langle 8\rangle 2.$ $\forall i, j \in [1..\#\mathcal{E}_{N_1} \circledS t''] : i < j \Rightarrow q.\mathcal{E}_{N_1} \circledS t''[i] < q.\mathcal{E}_{N_1} \circledS t''[j] \wedge$
$\#\mathcal{E}_{N_1} \circledS t'' = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.\mathcal{E}_{N_1} \circledS t''[i] > k$

Proof: By $\langle 8\rangle 1$, definition (7), and constraints (8) and (9), since the filtering of a trace with regard to a set of events does not change the ordering of the remaining events in the trace.

$\langle 8\rangle 3.$ Q.E.D.

Proof: By $\langle 6\rangle 3$, $\langle 8\rangle 2$ and the rule of replacement [51].

$\langle 7\rangle 2.$ $\forall i, j \in [1..\#t_2] : i < j \Rightarrow q.t_2[i] < q.t_2[j] \wedge$
$\#t_2 = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t_2[i] > k$

Proof: Symmetrical to step $\langle 7\rangle 1$

$\langle 7\rangle 3.$ Q.E.D.

Proof: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\wedge$ -introduction.

$\langle 6\rangle 8.$ $\{q.t_1[i] \mid i \in [1..\#t_1]\} \cap \{q.t_2[j] \mid j \in [1..\#t_2]\} = \emptyset$

Proof: By the assumption that each interface, and hence each component, is assigned a set of time-stamps disjoint from the set of time-stamps assigned to every other interface or component.

$\langle 6\rangle 9.$ $\Pi_{\{1,2\}}.(\Pi_{\{2\}}.((\{?\} \times \mathcal{M}) \circledS t_1)) \sqsubseteq \Pi_{\{1,2\}}.(\Pi_{\{2\}}.(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

Proof: By $\langle 6\rangle 4$ and constraint (11).

$\langle 6\rangle 10.$ $\Pi_{\{1,2\}}.(\Pi_{\{2\}}.((\{?\} \times \mathcal{M}) \circledS t_2)) \sqsubseteq \Pi_{\{1,2\}}.(\Pi_{\{2\}}.(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha))$

Proof: By $\langle 6\rangle 4$ and constraint (11).

$\langle 6\rangle 11.$ $\exists t''' \in \mathcal{H} : \mathcal{E}_{N_1} \circledS t''' = t_1 \wedge \mathcal{E}_{N_2} \circledS t''' = t_2$

Proof: By $\langle 6\rangle 7$ t_1 and t_2 fulfil well-formedness constraints (8) and (9) with regard to time. By $\langle 6\rangle 8$ their sets of time-stamps are disjoint. Hence, it is possible to interleave the events of t_1 and t_2 in such a way that the well-formedness constraints (8) and (9) are fulfilled. Furthermore, by $\langle 6\rangle 9$ the sequence of consumed messages in t_1 is a prefix of the messages in $\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha$ when disregarding time, and vice versa for t_2 by $\langle 6\rangle 10$. By $\langle 6\rangle 6$ the sequence of messages transmitted from N_1 to N_2 in t_1 is a prefix of the messages transmitted from N_1 to N_2 in α, and vice versa for t_2. Hence, it is possible to interleave the events of t_1 and t_2 in such a way that the sequence of consumed messages sent from N_1 to N_2, is a prefix of the sequence of transmitted messages from N_1 to N_2, and vice versa, when disregarding time, fulfilling constraint (10).

⟨6⟩12. Let: $t''' \in \mathcal{H}$ such that $\mathcal{E}_{N_1} \circledS t''' = t_1 \wedge \mathcal{E}_{N_2} \circledS t''' = t_2$
Proof: By ⟨6⟩11.

⟨6⟩13. $t''' \in \mathcal{H}_{N_1 \cup N_2}$
Proof: By ⟨6⟩12, ⟨6⟩5 and elementary set theory.

⟨6⟩14. $(\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS t''' \sqsubseteq (\{!\} \times \mathcal{S} \times N_2 \times N_1 \times \mathcal{Q}) \circledS \alpha \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t''' \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

⟨7⟩1. $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \mathcal{E}_{N_1} \circledS t''' \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha \wedge$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \mathcal{E}_{N_2} \circledS t''' \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
Proof:By ⟨6⟩12, ⟨6⟩6 and the rule of replacement [51].

⟨7⟩2. Q.E.D.
Proof:By ⟨7⟩1 and definition (7).

⟨6⟩15. $\mathcal{E}_{N_1} \circledS t''' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_2} \circledS t''' \in D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$
Proof: By ⟨6⟩12, ⟨6⟩4 and the rule of replacement.

⟨6⟩16. $t''' \in D_{N_1} \otimes D_{N_2}(\alpha)$
Proof: By ⟨6⟩13, ⟨6⟩14, ⟨6⟩15 and definition (22).

⟨6⟩17. Q.E.D.
Proof: By ⟨6⟩16, ⟨6⟩12 and $\exists$ -introduction.

⟨5⟩2. Q.E.D.
Proof: $\Rightarrow$-introduction.

⟨4⟩2. Q.E.D.
Proof: $\forall$-introduction

⟨3⟩2. Case: $t = t''' \frown \langle e \rangle$ (induction step)

⟨4⟩1. Assume: $(\forall t_1, t_2 \in \mathcal{H} \cap \mathcal{E}^* : t_1 \in \mathcal{E}_{N_1} \circledS c(t''', D_{N_1} \otimes D_{N_2}(\alpha)) \wedge$
$t_2 \in \mathcal{E}_{N_2} \circledS c(t''', D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$
$(\exists t' \in c(t''', D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2)$
(induction hypothesis)
Prove: $(\forall t_1, t_2 \in \mathcal{H} : t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge$
$t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$
$(\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2)$
(induction step)

⟨5⟩1. Assume: $t_1 \in \mathcal{H} \wedge t_2 \in \mathcal{H}$
Prove: $(t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$
$\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

⟨6⟩1. Assume: $t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

⟨7⟩1. Assume: $\neg \exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$
Prove: $\perp$

⟨8⟩1. $\exists t' \in c(t''', D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

⟨9⟩1. $t_1 \in \mathcal{E}_{N_1} \circledS c(t''', D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t''', D_{N_1} \otimes D_{N_2}(\alpha))$

⟨10⟩1. $c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq c(t''', D_{N_1} \otimes D_{N_2}(\alpha))$
Proof: By assumption ⟨3⟩2 and Lemma B.5.

⟨10⟩2. Q.E.D.

PROOF: By assumption $\langle 6\rangle 1$, $\langle 10\rangle 1$, definition (7) and elementary set theory.

$\langle 9\rangle 2$. Q.E.D.

PROOF: By $\langle 9\rangle 1$ and the induction hypothesis (assumption $\langle 4\rangle 1$).

$\langle 8\rangle 2$. LET: $t' \in c(t''', D_{N_1} \otimes D_{N_2}(\alpha))$ such that
$\mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

PROOF: By $\langle 8\rangle 1$.

$\langle 8\rangle 3$. $t' \notin c(t, D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By $\langle 8\rangle 2$ and assumption $\langle 7\rangle 1$.

$\langle 8\rangle 4$. $t \not\sqsubseteq t'$

PROOF: By $\langle 8\rangle 3$ and Definition 3.1.

$\langle 8\rangle 5$. $t \sqsubseteq t'$

$\langle 9\rangle 1$. $\mathcal{E}_{N_1} \circledS t \sqsubseteq t_1 \wedge \mathcal{E}_{N_2} \circledS t \sqsubseteq t_1$

PROOF: By assumption $\langle 6\rangle 1$, Definition 3.1 and definition (7).

$\langle 9\rangle 2$. $\mathcal{E}_{N_1} \circledS t \sqsubseteq \mathcal{E}_{N_1} \circledS t' \wedge \mathcal{E}_{N_2} \circledS t \sqsubseteq \mathcal{E}_{N_2} \circledS t'$

PROOF: By $\langle 9\rangle 1$, $\langle 8\rangle 2$ and the rule of replacement [51].

$\langle 9\rangle 3$. $\mathsf{rng}.t = \mathcal{E}_{N_1} \cup \mathcal{E}_{N_2}$

PROOF: By $\langle 8\rangle 2$, Definition 3.1, definition (22) and definition (20).

$\langle 9\rangle 4$. $\mathsf{rng}.t' = \mathcal{E}_{N_1} \cup \mathcal{E}_{N_2}$

PROOF: By assumption $\langle 2\rangle 1$, Definition 3.1, definition (22) and definition (20).

$\langle 9\rangle 5$. Q.E.D.

PROOF: By $\langle 9\rangle 2$, $\langle 9\rangle 3$, $\langle 9\rangle 4$ and constraint (8) which ensures that events in a trace are totally ordered by time.

$\langle 8\rangle 6$. Q.E.D.

PROOF: By $\langle 8\rangle 5$, $\langle 8\rangle 4$ and $\perp$-introduction.

$\langle 7\rangle 2$. Q.E.D.

PROOF: Proof by contradiction

$\langle 6\rangle 2$. Q.E.D.

PROOF: $\Rightarrow$-introduction.

$\langle 5\rangle 2$. Q.E.D.

PROOF: $\forall$-introduction.

$\langle 4\rangle 2$. Q.E.D.

PROOF: Induction step.

$\langle 3\rangle 3$. Q.E.D.

PROOF: By induction over the length of t with $\langle 3\rangle 1$ as basis step and $\langle 3\rangle 2$ as induction step.

$\langle 2\rangle 2$. Q.E.D.

PROOF: $\Rightarrow$-introduction.

$\langle 1\rangle 2$. Q.E.D.

PROOF: $\forall$-introduction.

Lemma B.23. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$\begin{aligned}\forall t_1 \in \mathcal{H} \cap \mathcal{E}^* :& (c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))\\ &\wedge \exists t \in \mathcal{H} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha\end{aligned}$$

$\wedge\, t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \wedge t \notin \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$

$(\#t > \#(\mathcal{E}_{N_1} \circledS t_1) \wedge q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1])$

Proof:

⟨1⟩1. Assume: $t_1 \in \mathcal{H} \cap \mathcal{E}^*$
Prove: $(c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge\, \exists t \in \mathcal{H} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
$\wedge t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \wedge t \notin \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow (\#t >$
$\#(\mathcal{E}_{N_1} \circledS t_1) \wedge q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1])$

⟨2⟩1. Assume: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge\, \exists t \in \mathcal{H} : (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$
$\wedge\, t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \wedge t \notin \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $\#t > \#(\mathcal{E}_{N_1} \circledS t_1) \wedge q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1]$

⟨3⟩1. Let: $t \in \mathcal{H}$ such that $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha \wedge t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \wedge \mathcal{E}_{N_1} \circledS t \notin$
$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$
Proof: By assumption ⟨2⟩1.

⟨3⟩2. Assume: $\#t \leq \#(\mathcal{E}_{N_1} \circledS t_1) \vee q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] \geq q.t_1[\#t_1]$
Prove: $\perp$

⟨4⟩1. $\mathcal{E}_{N_1} \circledS t_1 \sqsubseteq t$
Proof: By ⟨3⟩1 ($t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$) and Definition 3.1.

⟨4⟩2. $\exists t' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t = \mathcal{E}_{N_1} \circledS t'$

⟨5⟩1. $\exists t' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : \exists t'' \in D_{N_1} \otimes D_{N_2}(\alpha) : \mathcal{E}_{N_2} \circledS t'' = \mathcal{E}_{N_2} \circledS t' \wedge$
$\mathcal{E}_{N_1} \circledS t'' = t$

⟨6⟩1. $t \in \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$

⟨7⟩1. $t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
Proof: By ⟨3⟩1 ($t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$) and Definition 3.1.

⟨7⟩2. Q.E.D.
Proof: By ⟨3⟩1 ($(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$), ⟨7⟩1 and definition (22).

⟨6⟩2. $\forall t \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_2} \circledS t \in \mathcal{E}_{N_2} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$

⟨7⟩1. $\forall t \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t \in (D_{N_1} \otimes D_{N_2}(\alpha))$
Proof: By Definition 3.1.

⟨7⟩2. $\forall t \in (D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_2} \circledS t \in \mathcal{E}_{N_2} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$
Proof: By definition (22).

⟨7⟩3. Q.E.D.
Proof: By ⟨7⟩1 and ⟨7⟩2.

⟨6⟩3. Q.E.D.
Proof: By ⟨6⟩1, ⟨6⟩2, Lemma B.22 and $\exists$ introduction.

⟨5⟩2. Let: $t' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$ such that $\exists t'' \in D_{N_1} \otimes D_{N_2}(\alpha) : \mathcal{E}_{N_2} \circledS t'' =$
$\mathcal{E}_{N_2} \circledS t' \wedge \mathcal{E}_{N_1} \circledS t'' = t$
Proof: By ⟨5⟩1.

⟨5⟩3. Let: $t'' \in D_{N_1} \otimes D_{N_2}(\alpha)$ such that $\mathcal{E}_{N_2} \circledS t'' = \mathcal{E}_{N_2} \circledS t' \wedge \mathcal{E}_{N_1} \circledS t'' = t$
Proof: By ⟨5⟩2.

⟨5⟩4. $t'' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

⟨6⟩1. $t_1 \sqsubseteq t''$

⟨7⟩1. $\forall k \in [0..q.t_1[\#t_1]] : t''{\downarrow_k} = t_1{\downarrow_k}$

$\langle 8\rangle 1.$ $\forall k \in [0..q.t_1[\#t_1]] : \mathcal{E}_{N_1} \circledS t''{\downarrow_k} = \mathcal{E}_{N_1} \circledS t_1{\downarrow_k}$

$\langle 9\rangle 1.$ Case: $\#t \leq \#(\mathcal{E}_{N_1} \circledS t_1)$

$\langle 10\rangle 1.$ $\mathcal{E}_{N_1} \circledS t'' = \mathcal{E}_{N_1} \circledS t_1$

$\langle 11\rangle 1.$ $t = \mathcal{E}_{N_1} \circledS t_1$

Proof: By $\langle 4\rangle 1$ and assumption $\langle 9\rangle 1$.

$\langle 11\rangle 2.$ Q.E.D.

Proof: By $\langle 11\rangle 1$, $\langle 5\rangle 3$ and the rule of replacement [51].

$\langle 10\rangle 2.$ Q.E.D.

Proof: By $\langle 10\rangle 1$.

$\langle 9\rangle 2.$ Case: $q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] \geq q.t_1[\#t_1]$

$\langle 10\rangle 1.$ Assume: $\exists k \in [0..q.t_1[\#t_1]] : \mathcal{E}_{N_1} \circledS t''{\downarrow_k} \neq \mathcal{E}_{N_1} \circledS t_1{\downarrow_k}$

Prove: $\perp$

$\langle 11\rangle 1.$ $\forall i, j \in [1..\#t_1] : i < j \Rightarrow q.t_1[i] < q.t_1[j]$

Proof: By assumption $\langle 1\rangle 1$ and requirement (8).

$\langle 11\rangle 2.$ $q.\mathcal{E}_{N_1} \circledS t''[\mathcal{E}_{N_1} \circledS \#t_1 + 1] \geq q.t_1[\#t_1]$

Proof: By assumption $\langle 9\rangle 2$ and $\langle 5\rangle 3$.

$\langle 11\rangle 3.$ $\forall k \in [0..q.\mathcal{E}_{N_1} \circledS t_1[\#(\mathcal{E}_{N_1} \circledS t_1)]] : \mathcal{E}_{N_1} \circledS t''{\downarrow_k} = \mathcal{E}_{N_1} \circledS t_1{\downarrow_k}$

$\langle 12\rangle 1.$ $\mathcal{E}_{N_1} \circledS t_1 \sqsubseteq \mathcal{E}_{N_1} \circledS t''$

Proof: By $\langle 5\rangle 3$, $\langle 4\rangle 1$ and the rule of replacement [51].

$\langle 12\rangle 2.$ Q.E.D.

Proof: By $\langle 12\rangle 1$.

$\langle 11\rangle 4.$ Let: $k \in [0..q.t_1[\#t_1]]$ such that $\mathcal{E}_{N_1} \circledS t''{\downarrow_k} \neq \mathcal{E}_{N_1} \circledS t_1{\downarrow_k}$

Proof: By assumption $\langle 10\rangle 1$.

$\langle 11\rangle 5.$ $q.\mathcal{E}_{N_1} \circledS t_1[\#(\mathcal{E}_{N_1} \circledS t_1)] < k \leq q.t_1[\#t_1]$

Proof: By $\langle 11\rangle 1$, $\langle 11\rangle 2$, $\langle 11\rangle 3$ and $\langle 11\rangle 4$.

$\langle 11\rangle 6.$ $q.\mathcal{E}_{N_1} \circledS t''[\mathcal{E}_{N_1} \circledS \#t_1 + 1] < q.t_1[\#t_1]$

Proof: By $\langle 11\rangle 4$ and $\langle 11\rangle 5$.

$\langle 11\rangle 7.$ Q.E.D.

Proof: By $\langle 11\rangle 2$, $\langle 11\rangle 6$ and $\perp$ introduction.

$\langle 10\rangle 2.$ Q.E.D.

Proof: Proof by contradiction.

$\langle 9\rangle 3.$ Q.E.D.

Proof: The cases $\langle 9\rangle 1$ and $\langle 9\rangle 2$ are exhaustive.

$\langle 8\rangle 2.$ $\forall k \in [0..q.t_1[\#t_1]] : \mathcal{E}_{N_2} \circledS t''{\downarrow_k} = \mathcal{E}_{N_2} \circledS t_1{\downarrow_k}$

$\langle 9\rangle 1.$ $\forall k \in [0..q.t_1[\#t_1]] : \mathcal{E}_{N_2} \circledS t'{\downarrow_k} = \mathcal{E}_{N_2} \circledS t_1{\downarrow_k}$

$\langle 10\rangle 1.$ $t_1 \sqsubseteq t'$

Proof: By $\langle 5\rangle 2$ and Definition 3.1.

$\langle 10\rangle 2.$ Q.E.D.

Proof: By $\langle 10\rangle 1$, since otherwise t' would not be well-formed.

$\langle 9\rangle 2.$ Q.E.D.

Proof: By $\langle 5\rangle 3$, $\langle 9\rangle 1$ and the rule of replacement.

$\langle 8\rangle 3.$ $\mathsf{rng}.t'' \subseteq \mathcal{E}_{N_1} \cup \mathcal{E}_{N_2}$

Proof: By $\langle 5\rangle 3$, Definition 5.3, definition (20) and definition (5).

$\langle 8\rangle 4.$ $\mathsf{rng}.t_1 \subseteq \mathcal{E}_{N_1} \cup \mathcal{E}_{N_2}$

Proof: By assumption $\langle 2\rangle 1$, Definition 3.1, Definition 5.3, definition (20) and definition (5).

$\langle 8\rangle 5.$ Q.E.D.

Proof: By $\langle 8\rangle 1$, $\langle 8\rangle 2$, $\langle 8\rangle 3$ and $\langle 8\rangle 4$.

$\langle 7\rangle 2.$ Q.E.D.

Proof: By $\langle 7\rangle 1$.

$\langle 6\rangle 2.$ Q.E.D.

Proof: By $\langle 5\rangle 3$, $\langle 6\rangle 1$ and Definition 3.1.

$\langle 5\rangle 5.$ Q.E.D.

Proof: By $\langle 5\rangle 3$, $\langle 5\rangle 4$ and the rule of replacement

$\langle 4\rangle 3.$ $\neg\exists t' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t = \mathcal{E}_{N_1} \circledS t'$

Proof: By $\langle 3\rangle 1$ and definition (7).

$\langle 4\rangle 4.$ Q.E.D.

Proof: By $\langle 4\rangle 2$, $\langle 4\rangle 3$ and $\perp$ introduction.

$\langle 3\rangle 3.$ Q.E.D.

Proof: Proof by contradiction.

$\langle 2\rangle 2.$ Q.E.D.

Proof: $\Rightarrow$ introduction.

$\langle 1\rangle 2.$ Q.E.D.

Proof: $\forall$ introduction.

Lemma B.24. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$\forall t_1 \in \mathcal{H} \cap \mathcal{E}^* : \#t_1 > 1 \wedge c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$$
$$(c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \setminus \bigcup_{t \in T} c(t, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) =$$
$$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$$
where $T = \{t \in \mathcal{H} \mid \#t = \#(\mathcal{E}_{N_1} \circledS t_1) + 1 \wedge \exists t' \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) : t \sqsubseteq t' \wedge$
$q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1]\}$

Proof:

$\langle 1\rangle 1.$ Assume: $t_1 \in \mathcal{H} \cap \mathcal{E}^* \wedge \#t_1 > 1$
Let: $T = \{t \in \mathcal{H} \mid \#t = \#(\mathcal{E}_{N_1} \circledS t_1) + 1 \wedge \exists t' \in D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) : t \sqsubseteq t' \wedge$
$q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1]\}$
Prove: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$
$(c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \setminus \bigcup_{t'' \in T} c(t'', D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) =$
$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)))$

$\langle 2\rangle 1.$ Assume: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $(c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \setminus \bigcup_{t'' \in T} c(t'', D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) =$
$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 3\rangle 1.$ $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)))$
$\subseteq (c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \setminus \bigcup_{t'' \in T} c(t'', D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha))$

$\langle 4\rangle 1.$ Assume: $t \in \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$
Prove: $t \in (c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \wedge t \notin \bigcup_{t'' \in T} c(t'', D_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha))$

$\langle 5\rangle 1.$ $\forall t \in \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) :$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

$\langle 6\rangle 1.$ $\forall t \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) :$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

⟨7⟩1. $\forall t \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t \in D_{N_1} \otimes D_{N_2}(\alpha)$

Proof: By assumption ⟨2⟩1 and Definition 3.1.

⟨7⟩2. $\forall t \in D_{N_1} \otimes D_{N_2}(\alpha) :$
$(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

Proof: By definition (22).

⟨7⟩3. Q.E.D.

Proof: By ⟨7⟩1 and ⟨7⟩2.

⟨6⟩2. Q.E.D.

Proof: By ⟨6⟩1 and definition (7).

⟨5⟩2. $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

Proof: By assumption ⟨1⟩1, assumption ⟨2⟩1 and Lemma B.21.

⟨5⟩3. $t \in c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)$

Proof: By ⟨5⟩1, definition (24) and ⟨5⟩2.

⟨5⟩4. $t \notin \bigcup_{t'' \in T} c(t'', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

⟨6⟩1. Assume: $t \in \bigcup_{t'' \in T} c(t'', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$
Prove: $\perp$

⟨7⟩1. $\exists t' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t = \mathcal{E}_{N_1} \circledS t'$

Proof: By assumption ⟨4⟩1 and definition (7).

⟨7⟩2. Let: $t' \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$ such that $t = \mathcal{E}_{N_1} \circledS t'$

Proof: By ⟨7⟩1.

⟨7⟩3. $t' \in \mathcal{H}$

Proof: By ⟨7⟩2 and Definition 3.1.

⟨7⟩4. $t_1 \sqsubseteq t'$

Proof: By ⟨7⟩2 and Definition 3.1.

⟨7⟩5. $q.\mathcal{E}_{N_1} \circledS t'[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t'[\#t_1]$

⟨8⟩1. $t'[\#t_1] = t_1[\#t_1]$

Proof: By ⟨7⟩4 and definition (2).

⟨8⟩2. $q.\mathcal{E}_{N_1} \circledS t'[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1]$

⟨9⟩1. $q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1]$

Proof: By assumption ⟨6⟩1 and assumption ⟨1⟩1.

⟨9⟩2. Q.E.D.

Proof: By ⟨9⟩1, ⟨7⟩2 and the rule of replacement.

⟨8⟩3. Q.E.D.

Proof: By ⟨8⟩1, ⟨8⟩2 and the rule of replacement [51].

⟨7⟩6. $\exists j \in [\#t_1 + 1..\#t'] : t'[j] = \mathcal{E}_{N_1} \circledS t'[\#(\mathcal{E}_{N_1} \circledS t_1) + 1]$

⟨8⟩1. $\#(\mathcal{E}_{N_1} \circledS t') > \#(\mathcal{E}_{N_1} \circledS t_1)$

Proof: By assumption ⟨6⟩1, assumption ⟨1⟩1, ⟨7⟩2 and the rule of replacement.

⟨8⟩2. Q.E.D.

Proof: By ⟨7⟩4, ⟨8⟩1 and ⟨7⟩3, since by constraint (8) any event in $\mathsf{rng}.t' \cap \mathcal{E}_{N_1}$ not in $\mathsf{rng}.t_1$ must occur after $t'[\#t_1]$ in t'.

⟨7⟩7. Let: $j \in [\#t_1 + 1..\#t']$ such that $t'[j] = \mathcal{E}_{N_1} \circledS t'[\#(\mathcal{E}_{N_1} \circledS t_1) + 1]$

Proof: By ⟨7⟩6

⟨7⟩8. $q.t'[j] < q.t'[\#t_1]$

Proof: By ⟨7⟩5, ⟨7⟩7 and the fact that every event in a trace is unique, due to the total ordering of events by time (constraint (8)).

$\langle 7\rangle 9.$ $t' \notin \mathcal{H}$

Proof: By $\langle 7\rangle 7$, $\langle 7\rangle 8$ and constraint (8).

$\langle 7\rangle 10.$ Q.E.D.

Proof: By $\langle 7\rangle 3$, $\langle 7\rangle 9$ and $\perp$-introduction.

$\langle 6\rangle 2.$ Q.E.D.

Proof: Proof by contradiction.

$\langle 5\rangle 5.$ Q.E.D.

Proof: By $\langle 5\rangle 3$, $\langle 5\rangle 4$ and $\wedge$-introduction.

$\langle 3\rangle 2.$ $(c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1-N_2}(\alpha)) \setminus \bigcup_{t''\in T} c(t'', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \subseteq \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 4\rangle 1.$ Assume: $t \in (c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1-N_2}(\alpha)) \setminus \bigcup_{t''\in T} c(t'', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

Prove: $t \in \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 5\rangle 1.$ Assume: $t \notin \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

Prove: $\perp$

$\langle 6\rangle 1.$ $(\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS t \sqsubseteq (\{!\} \times \mathcal{S} \times N_1 \times N_2 \times \mathcal{Q}) \circledS \alpha$

Proof: By assumption $\langle 4\rangle 1$ ($t \in CT_{N_1-N_2}(\alpha)$) and definition (24).

$\langle 6\rangle 2.$ $(\#t > \#(\mathcal{E}_{N_1} \circledS t_1)) \wedge (q.t[\#\mathcal{E}_{N_1} \circledS t_1 + 1] < q.t_1[\#t_1])$

Proof: By assumption $\langle 1\rangle 1$, assumption $\langle 2\rangle 1$, assumption $\langle 4\rangle 1$, assumption $\langle 5\rangle 1$, $\langle 6\rangle 1$ and Lemma B.23.

$\langle 6\rangle 3.$ $t \in \bigcup_{t''\in T} c(t'', D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

Proof: By $\langle 6\rangle 2$ and $\langle 1\rangle 1$.

$\langle 6\rangle 4.$ Q.E.D.

Proof: By assumption $\langle 4\rangle 1$, $\langle 6\rangle 3$ and $\perp$-introduction.

$\langle 5\rangle 2.$ Q.E.D.

Proof: Proof by contradiction.

$\langle 4\rangle 2.$ Q.E.D.

Proof: $\subseteq$ rule.

$\langle 3\rangle 3.$ Q.E.D.

Proof: By $\langle 3\rangle 1$, $\langle 3\rangle 2$ and the $=$-rule for sets [29].

$\langle 2\rangle 2.$ Q.E.D.

Proof: $\Rightarrow$-introduction.

$\langle 1\rangle 2.$ Q.E.D.

Proof: $\forall$-introduction.

Lemma B.25. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1-N_2}(\alpha) = \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$$

Proof:

$\langle 1\rangle 1.$ $D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1-N_2}(\alpha) = \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 2\rangle 1.$ $D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1-N_2}(\alpha) \subseteq \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 3\rangle 1.$ Assume: $t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge t \in CT_{N_1-N_2}(\alpha)$

Prove: $t \in \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 4\rangle 1.$ Q.E.D.

Proof: By assumption $\langle 3\rangle 1$, definition (22), definition (24) and definition (7).

⟨3⟩2. Q.E.D.

PROOF: $\subseteq$ rule.

⟨2⟩2. $\mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1-N_2}(\alpha)$

⟨3⟩1. ASSUME: $t \in \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$
PROVE: $t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge t \in CT_{N_1-N_2}(\alpha)$

⟨4⟩1. $\exists t' \in D_{N_1} \otimes D_{N_2}(\alpha) : t = \mathcal{E}_{N_1} \circledS t'$

PROOF: By assumption ⟨3⟩1 and definition (7).

⟨4⟩2. LET: $t' \in D_{N_1} \otimes D_{N_2}(\alpha)$ such that $t = \mathcal{E}_{N_1} \circledS t'$

PROOF: By ⟨4⟩1.

⟨4⟩3. $\mathcal{E}_{N_1} \circledS t' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

PROOF: By assumption ⟨3⟩1, ⟨4⟩2 and definition (22).

⟨4⟩4. $\mathcal{E}_{N_1} \circledS t' \in CT_{N_1-N_2}(\alpha)$

PROOF: By assumption ⟨3⟩1, ⟨4⟩2 and definition (24).

⟨4⟩5. Q.E.D.

PROOF: By ⟨4⟩3, ⟨4⟩4 and $\wedge$ -introduction.

⟨3⟩2. Q.E.D.

PROOF: $\subseteq$ rule.

⟨2⟩3. Q.E.D.

PROOF: By ⟨2⟩1, ⟨2⟩2 and the =-rule for sets [29].

⟨1⟩2. Q.E.D.

Lemma B.26. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$\begin{aligned}\forall t_1 \in \mathcal{H} \cap \mathcal{E}^* : & c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow \\ & (\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \\ & (\mathcal{E}_{N_2} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)\end{aligned}$$

PROOF:

⟨1⟩1. ASSUME: $t_1 \in \mathcal{H} \cap \mathcal{E}^*$
PROVE: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha)) \Rightarrow$
$(\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge$
$(\mathcal{E}_{N_2} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

⟨2⟩1. ASSUME: $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \in C(D_{N_1} \otimes D_{N_2}(\alpha))$
PROVE: $(\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge$
$(\mathcal{E}_{N_2} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

⟨3⟩1. $(\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

⟨4⟩1. CASE: $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) = \emptyset$

⟨5⟩1. Q.E.D.

PROOF: Since $\emptyset \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ by Definition 5.2 and Definition 5.3.

⟨4⟩2. CASE: $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \neq \emptyset$

⟨5⟩1. $c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

⟨6⟩1. $\exists t' \in D_{N_1} \otimes D_{N_2}(\alpha) : \mathcal{E}_{N_1} \circledS t' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_1} \circledS t_1 \sqsubseteq \mathcal{E}_{N_1} \circledS t'$

⟨7⟩1. $\forall t \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) : t \in D_{N_1} \otimes D_{N_2}(\alpha) \wedge t_1 \sqsubseteq t$

PROOF: By assumption ⟨2⟩1, Definition 3.2 and Definition 3.1.

⟨7⟩2. $\forall t \in D_{N_1} \otimes D_{N_2}(\alpha) : \mathcal{E}_{N_1} \circledS t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

PROOF: By definition (22).

⟨7⟩3. LET: $t \in c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

⟨7⟩4. $t \in D_{N_1} \otimes D_{N_2}(\alpha) \wedge \mathcal{E}_{N_1} \circledS t \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_1} \circledS t_1 \sqsubseteq \mathcal{E}_{N_1} \circledS t$

PROOF: By ⟨7⟩1, ⟨7⟩2, ⟨7⟩3 and $\forall$ elimination.

⟨7⟩5. Q.E.D.

PROOF: By ⟨7⟩4 and $\exists$-introduction.

⟨6⟩2. Q.E.D.

PROOF: By ⟨6⟩1 and Definition 3.1.

⟨5⟩2. CASE: $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) = c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

⟨6⟩1. Q.E.D.

PROOF: By ⟨5⟩1 and assumption ⟨5⟩2.

⟨5⟩3. CASE: $\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) \neq c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha))$

⟨6⟩1. $CT_{N_1 - N_2}(\alpha) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

PROOF: By Lemma 5.4.

⟨6⟩2. $c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

PROOF: By ⟨5⟩1 and ⟨6⟩1, since $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ is closed under countable intersection.

⟨6⟩3. CASE: $t_1 = \langle\rangle$

⟨7⟩1. $c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha) = \mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

⟨8⟩1. $c(t_1, D_{N_1} \otimes D_{N_2}(\alpha)) = D_{N_1} \otimes D_{N_2}(\alpha)$

PROOF: By assumption ⟨6⟩3 and Definition 3.1.

⟨8⟩2. $c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) = D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

PROOF: By assumption ⟨6⟩3, definition (7) and Definition 3.1.

⟨8⟩3. Q.E.D.

PROOF: By ⟨8⟩1, ⟨8⟩2 and Lemma B.25.

⟨7⟩2. Q.E.D.

PROOF: By ⟨6⟩2, ⟨7⟩1 and the rule of replacement [51].

⟨6⟩4. CASE: $t_1 \neq \langle\rangle$

⟨7⟩1. LET: $T = \{t \in \mathcal{H} \mid \#t = \#(\mathcal{E}_{N_1} \circledS t_1) + 1 \wedge \exists t' \in D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) :$
$t \sqsubseteq t' \wedge q.t[\#(\mathcal{E}_{N_1} \circledS t_1) + 1] < q.t_1[\#t_1]\}$

⟨7⟩2. $(c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \setminus \bigcup_{t \in T} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) =$
$\mathcal{E}_{N_1} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By assumption ⟨1⟩1 assumption ⟨2⟩1, ⟨7⟩1 and Lemma B.24.

⟨7⟩3. $(c(\mathcal{E}_{N_1} \circledS t_1, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \cap CT_{N_1 - N_2}(\alpha)) \setminus \bigcup_{t \in T} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \in$
$\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

⟨8⟩1. $\bigcup_{t \in T} c(t, D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$

PROOF: By assumption ⟨1⟩1, ⟨7⟩1 and Corollary B.10.

⟨8⟩2. Q.E.D.

PROOF: By ⟨6⟩2 and ⟨8⟩1, since $\mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$ is closed under set-difference.

⟨7⟩4. Q.E.D.

PROOF: By ⟨7⟩3, ⟨7⟩2 and the rule of replacement [51].

⟨6⟩5. Q.E.D.

PROOF: The cases ⟨6⟩3 and ⟨6⟩4 are exhaustive.

⟨5⟩4. Q.E.D.

PROOF: The cases ⟨5⟩2 and ⟨5⟩3 are exhaustive.

$\langle 4\rangle 3.$ Q.E.D.

PROOF: The cases $\langle 4\rangle 1$ and $\langle 4\rangle 2$ are exhaustive.

$\langle 3\rangle 2.$ $(\mathcal{E}_{N_2} \circledS c(t_1, D_{N_1} \otimes D_{N_2}(\alpha))) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

PROOF: Symmetrical to $\langle 3\rangle 1$.

$\langle 3\rangle 3.$ Q.E.D.

PROOF: By $\langle 3\rangle 1$, $\langle 3\rangle 2$ and $\wedge$ -introduction.

$\langle 2\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$-introduction.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\forall$-introduction.

Theorem 5.5 *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$, let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$ and let $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ be a measure on $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as defined by (25). Then the function $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ is well defined. That is:*

$$\forall c \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)) : (\mathcal{E}_{N_1} \circledS c) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge (\mathcal{E}_{N_2} \circledS c) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$$

PROOF. Follows from Lemma B.16 and Lemma B.26.

Lemma B.27. *Let $(D_1, \mathcal{F}_1, \mu_1)$ and $(D_2, \mathcal{F}_2, \mu_2)$ be measure spaces. Then*

$$\begin{aligned}
&\forall A_1 \in \mathcal{F}_1, A_2 \in \mathcal{F}_2 : \\
&\qquad (\forall \phi \in (\mathbb{P}(D_1 \times D_2))^{\omega} : \forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2 \\
&\qquad \wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset) \\
&\qquad \wedge \bigcup_{i=1}^{\#\phi} \phi[i] = A_1 \times A_2 \wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2) \\
&\qquad \Rightarrow (\mu_1(A_1) \cdot \mu_2(A_2) = \sum_{i=1}^{\#\phi} \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\}))^8
\end{aligned}$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $A_1 \in \mathcal{F}_1 \wedge A_2 \in \mathcal{F}_2 :$

PROVE: $(\forall \phi \in (\mathbb{P}(D_1 \times D_2))^{\omega} : \forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2$
$\wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] = A_1 \times A_2 \wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2)$
$\Rightarrow (\mu_1(A_1) \cdot \mu_2(A_2) = \sum_{i=1}^{\#\phi} \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\}))$

$\langle 2\rangle 1.$ ASSUME: $\phi \in (\mathbb{P}(D_1 \times D_2))^{\omega}$

PROVE: $\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2$
$\wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] = A_1 \times A_2 \wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2 \Rightarrow$
$\mu_1(A_1) \cdot \mu_2(A_2) = \sum_{i=1}^{\#\phi} \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\})$

$\langle 3\rangle 1.$ ASSUME: $i \in [1..\#\phi]$

[8] $D_1 \times D_2$ denotes the cartesian product of D_1 and D_2, and $\mathcal{F}_1 \overline{\times} \mathcal{F}_2$ denotes the product σ-field, that is, is the smallest σ-field containing all measurable rectangles of $D_1 \times D_2$, as defined in Definition A.10.

PROVE: $\phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2 \wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] = A_1 \times A_2 \wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2 \Rightarrow$
$\mu_1(A_1) \cdot \mu_2(A_2) = \sum_{i=1}^{\#\phi} \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\})$

$\langle 4 \rangle 1.$ ASSUME: $\phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2 \wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] = A_1 \times A_2 \wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2$
PROVE: $\mu_1(A_1) \cdot \mu_2(A_2) = \sum_{i=1}^{\#\phi} \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\})$

$\langle 5 \rangle 1.$ There is a unique measure μ on $\mathcal{F}_1 \overline{\times} \mathcal{F}_2$, such that
$\mu_1(A_1) \cdot \mu_2(A_2) = \mu(\bigcup_{i=1}^{\#\phi} \phi[i])$
PROOF: By assumption $\langle 1 \rangle 1$, assumption $\langle 4 \rangle 1$ ($A_1 \times A_2 = \bigcup_{i=1}^{\#\phi} \phi[i]$) and Theorem B.4.

$\langle 5 \rangle 2.$ LET: μ be the unique measure μ on $\mathcal{F}_1 \overline{\times} \mathcal{F}_2$, such that
$\mu_1(A_1) \cdot \mu_2(A_2) = \mu(\bigcup_{i=1}^{\#\phi} \phi[i])$
PROOF: By $\langle 5 \rangle 1$.

$\langle 5 \rangle 3.$ $\mu(\bigcup_{i=1}^{\#\phi} \phi[i]) = \sum_{i=1}^{\#\phi} \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\})$

$\langle 6 \rangle 1.$ $\mu(\bigcup_{i=1}^{\#\phi} \phi[i]) = \sum_{i=1}^{\#\phi} \mu(\phi[i])$
PROOF: By Theorem B.4 μ is a measure on $\mathcal{F}_1 \overline{\times} \mathcal{F}_2$, which by Definition A.6 implies that it is countably additive.

$\langle 6 \rangle 2.$ $\forall i \in [1..\#\phi] : \mu(\phi[i]) = \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\})$

$\langle 7 \rangle 1.$ ASSUME: $i \in [1..\#\phi]$
PROVE: $\mu(\phi[i]) = \mu_1(\{\Pi_1.p \mid p \in \phi[i]\}) \cdot \mu_2(\{\Pi_2.p \mid p \in \phi[i]\})$

$\langle 8 \rangle 1.$ $\phi[i] = \{\Pi_1.p \mid p \in \phi[i]\} \times \{\Pi_2.p \mid p \in \phi[i]\}$
PROOF: By assumption $\langle 7 \rangle 1$, assumption $\langle 4 \rangle 1$ and definition (32).

$\langle 8 \rangle 2.$ $\{\Pi_1.p \mid p \in \phi[i]\} \in \mathcal{F}_1 \wedge \{\Pi_2.p \mid p \in \phi[i]\} \in \mathcal{F}_2$
PROOF: By assumption $\langle 7 \rangle 1$, $\langle 4 \rangle 1$ ($\phi[i] \in \mathcal{F}_1 \overline{\times} \mathcal{F}_2$) and definition (A.10).

$\langle 8 \rangle 3.$ Q.E.D.
PROOF: By $\langle 8 \rangle 1$, $\langle 8 \rangle 2$ and Theorem B.4.

$\langle 7 \rangle 2.$ Q.E.D.
PROOF: $\forall$-introduction.

$\langle 6 \rangle 3.$ Q.E.D.
PROOF: By $\langle 6 \rangle 1$ and $\langle 6 \rangle 2$.

$\langle 5 \rangle 4.$ Q.E.D.
PROOF: By $\langle 5 \rangle 2$, $\langle 5 \rangle 3$ and the rule of transitivity [51].

$\langle 4 \rangle 2.$ Q.E.D.
PROOF: $\Rightarrow$-introduction.

$\langle 3 \rangle 2.$ Q.E.D.
PROOF: $\forall$-introduction.

$\langle 2 \rangle 2.$ Q.E.D.
PROOF: $\forall$-introduction.

$\langle 1 \rangle 2.$ Q.E.D.
PROOF: $\forall$-introduction.

Lemma B.28. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Then*

$$\forall \phi \in \mathbb{P}(\mathcal{H})^{\omega} : (\forall i \in [1..\#\phi] : \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$$
$$\wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$$

$$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$$

$$\Rightarrow (\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi[i]))$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $\phi \in \mathbb{P}(\mathcal{H})^{\,\omega}$

PROVE: $(\forall i \in [1..\#\phi] : \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\Rightarrow (\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi[i]))$

$\langle 2\rangle 1.$ ASSUME: $\forall i \in [1..\#\phi] : \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

PROVE: $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi[i])$

$\langle 3\rangle 1.$ $\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

PROOF: By assumption $\langle 2\rangle 1$ and Theorem 5.5.

$\langle 3\rangle 2.$ $\forall i \in [1..\#\phi] : \mathcal{E}_{N_1} \circledS \phi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_2} \circledS \phi[i] \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

PROOF: By assumption $\langle 2\rangle 1$ and Theorem 5.5.

$\langle 3\rangle 3.$ $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) =$
$f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i])$

PROOF: By definition (25) and $\langle 3\rangle 1$.

$\langle 3\rangle 4.$ $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) =$
$\sum_{i=1}^{\#\phi} f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS \phi[i])$

$\langle 4\rangle 1.$ CASE: $\bigcup_{i=1}^{\#\phi} \phi[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \setminus C(D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 5\rangle 1.$ $\exists t \in (D_{N_1} \otimes D_{N_2}(\alpha) \cap \mathcal{E}^{\,*}) : \{t\} = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By assumption $\langle 4\rangle 1$ and Definition 3.3.

$\langle 5\rangle 2.$ LET: $t \in (D_{N_1} \otimes D_{N_2}(\alpha) \cap \mathcal{E}^{\,*})$ such that $\{t\} = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By $\langle 5\rangle 1$.

$\langle 5\rangle 3.$ $\#\phi = 1$

PROOF: By $\langle 5\rangle 2$ and assumption $\langle 2\rangle 1$.

$\langle 5\rangle 4.$ Q.E.D.

PROOF: By $\langle 5\rangle 3$.

$\langle 4\rangle 2.$ CASE: $\bigcup_{i=1}^{\#\phi} \phi[i] \in C(D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 5\rangle 1.$ LET: ψ be a sequence in $(\mathbb{P}(D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \times D_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)))^{\,\omega}$ such that
$\#\psi = \#\phi \wedge \forall i \in [1..\#\phi] : \psi[i] = \{(\mathcal{E}_{N_1} \circledS t, \mathcal{E}_{N_2} \circledS t) \,|\, t \in \phi[i]\}$

$\langle 5\rangle 2.$ $\forall i \in [1..\#\psi] : \psi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha) \wedge$
$(\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset) \wedge$
$\bigcup_{i=1}^{\#\psi} \psi[i] = \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \wedge$
$\bigcup_{i=1}^{\#\psi} \psi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha) \Rightarrow$
$(f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) =$
$\sum_{i=1}^{\#\psi} f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\{\Pi_1.p \,|\, p \in \psi[i]\}) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\{\Pi_2.p \,|\, p \in \psi[i]\})$

Proof: By $\langle 3\rangle 1$, $\langle 5\rangle 1$, the assumption that I_{N_1} and I_{N_2} are probabilistic component executions, Definition 5.3, Definition 3.4, Lemma B.27 and $\forall$ elimination.

$\langle 5\rangle 3.$ $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha)(\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS\, \alpha)(\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) =$
$\sum_{i=1}^{\#\psi} f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha)(\{\Pi_1.p \mid p \in \psi[i]\}) \cdot f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS\, \alpha)(\{\Pi_2.p \mid p \in \psi[i]\})$

$\langle 6\rangle 1.$ $\forall i \in [1..\#\psi] : \psi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS\, \alpha)$

$\langle 7\rangle 1.$ Assume: $i \in [1..\#\psi]$
Prove: $\psi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS\, \alpha)$

$\langle 8\rangle 1.$ $\psi[i] = \mathcal{E}_{N_1} \circledS\, \phi[i] \times \mathcal{E}_{N_2} \circledS\, \phi[i]$

Proof: By assumption $\langle 7\rangle 1$, $\langle 5\rangle 1$, definition (32) and definition (7).

$\langle 8\rangle 2.$ $\mathcal{E}_{N_1} \circledS\, \phi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha) \wedge \mathcal{E}_{N_2} \circledS\, \phi[i] \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS\, \alpha)$

Proof: By $\langle 3\rangle 2$, assumption $\langle 7\rangle 1$, $\langle 5\rangle 1$ and $\forall$ elimination.

$\langle 8\rangle 3.$ $\mathcal{E}_{N_1} \circledS\, \phi[i] \times \mathcal{E}_{N_2} \circledS\, \phi[i] \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS\, \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS\, \alpha)$

Proof: By $\langle 8\rangle 2$ and Definition A.10.

$\langle 8\rangle 4.$ Q.E.D.

Proof: By $\langle 8\rangle 1$, $\langle 8\rangle 3$ and the rule of replacement [51].

$\langle 7\rangle 2.$ Q.E.D.

Proof: $\forall$ introduction.

$\langle 6\rangle 2.$ $\forall l, m \in [1..\#\psi] : l \neq m \Rightarrow \psi[l] \cap \psi[m] = \emptyset$

Proof: By assumption $\langle 2\rangle 1$ and $\langle 5\rangle 1$.

$\langle 6\rangle 3.$ $\bigcup_{i=1}^{\#\psi} \psi[i] = \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]$

$\langle 7\rangle 1.$ $\bigcup_{i=1}^{\#\psi} \psi[i] \subseteq \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]$

$\langle 8\rangle 1.$ Assume: $p \in \bigcup_{i=1}^{\#\psi} \psi[i]$
Prove: $p \in \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]$

$\langle 9\rangle 1.$ $\exists t \in \bigcup_{i=1}^{\#\phi} \phi[i] : p = (\mathcal{E}_{N_1} \circledS\, t, \mathcal{E}_{N_2} \circledS\, t)$

Proof: By assumption $\langle 8\rangle 1$ and $\langle 5\rangle 1$.

$\langle 9\rangle 2.$ Let: $t \in \bigcup_{i=1}^{\#\phi} \phi[i]$ such that $p = (\mathcal{E}_{N_1} \circledS\, t, \mathcal{E}_{N_2} \circledS\, t)$

Proof: By $\langle 9\rangle 1$.

$\langle 9\rangle 3.$ $\mathcal{E}_{N_1} \circledS\, t \in \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \wedge \mathcal{E}_{N_2} \circledS\, t \in \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]$

Proof: By $\langle 9\rangle 2$ and definition (7).

$\langle 9\rangle 4.$ Q.E.D.

Proof: By $\langle 9\rangle 2$, $\langle 9\rangle 3$ and definition (32).

$\langle 8\rangle 2.$ Q.E.D.

Proof: $\subseteq$ rule

$\langle 7\rangle 2.$ $\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \subseteq \bigcup_{i=1}^{\#\psi} \psi[i]$

$\langle 8\rangle 1.$ Assume: $p \in \mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]$
Prove: $p \in \bigcup_{i=1}^{\#\psi} \psi[i]$

$\langle 9\rangle 1.$ $\exists t_1 \in (\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) : \exists t_2 \in (\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]) : p = (t_1, t_2)$

Proof: By assumption $\langle 8\rangle 1$ and definition (32).

$\langle 9\rangle 2.$ Let: $t_1 \in (\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i]), t_2 \in (\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i])$ such that
$p = (t_1, t_2)$

Proof: By $\langle 9\rangle 1$.

$\langle 9\rangle 3.$ $\exists t \in \bigcup_{i=1}^{\#\phi} \phi[i] : \mathcal{E}_{N_1} \circledS\, t = t_1 \wedge \mathcal{E}_{N_2} \circledS\, t = t_2$

$\langle 10\rangle 1.$ $\exists t \in \mathcal{H} \cap \mathcal{E}^* : \exists t' \in D_{N_1} \otimes D_{N_2}(\alpha) : t \sqsubseteq t' \wedge$

$c(t, D_{N_1} \otimes D_{N_2}(\alpha)) = \bigcup_{i=1}^{\#\phi} \phi[i]$

Proof: By assumption $\langle 4 \rangle 2$.

$\langle 10 \rangle 2$. Let: $t \in \mathcal{H} \cap \mathcal{E}^*$ such that $\exists t' \in D_{N_1} \otimes D_{N_2}(\alpha) : t \sqsubseteq t' \wedge$
$c(t, D_{N_1} \otimes D_{N_2}(\alpha)) = \bigcup_{i=1}^{\#\phi} \phi[i]$

Proof: By $\langle 10 \rangle 1$.

$\langle 10 \rangle 3$. $\forall t_1, t_2 \in \mathcal{H} : t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge$
$t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))) \Rightarrow$
$(\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2)$

Proof: By assumption $\langle 2 \rangle 1$, $\langle 10 \rangle 2$ the rule of replacement [51] and Lemma B.22.

$\langle 10 \rangle 4$. $t_1 \in \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge t_2 \in \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 11 \rangle 1$. $\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] = \mathcal{E}_{N_1} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha)) \wedge$
$\mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] = \mathcal{E}_{N_2} \circledS c(t, D_{N_1} \otimes D_{N_2}(\alpha))$

Proof: By $\langle 10 \rangle 2$ and the rule of equality between functions [51].

$\langle 11 \rangle 2$. Q.E.D.

Proof: By $\langle 9 \rangle 2$, $\langle 11 \rangle 1$ and the rule of replacement [51].

$\langle 10 \rangle 5$. $\exists t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha)) : \mathcal{E}_{N_1} \circledS t' = t_1 \wedge \mathcal{E}_{N_2} \circledS t' = t_2$

Proof: By $\langle 10 \rangle 3$, $\langle 10 \rangle 4$ and $\forall$ elimination.

$\langle 10 \rangle 6$. Let: $t' \in c(t, D_{N_1} \otimes D_{N_2}(\alpha))$ such that $\mathcal{E}_{N_1} \circledS t' = t_1 \wedge$
$\mathcal{E}_{N_2} \circledS t' = t_2$

Proof: By $\langle 10 \rangle 5$.

$\langle 10 \rangle 7$. $t' \in \bigcup_{i=1}^{\#\phi} \phi[i]$

Proof: By $\langle 10 \rangle 2$, $\langle 10 \rangle 6$ and the rule of replacement [51].

$\langle 10 \rangle 8$. Q.E.D.

Proof: By $\langle 10 \rangle 7$, $\langle 10 \rangle 6$ and $\exists$ introduction.

$\langle 9 \rangle 4$. Let: $t \in \bigcup_{i=1}^{\#\phi} \phi[i]$ such that $\mathcal{E}_{N_1} \circledS t = t_1 \wedge \mathcal{E}_{N_2} \circledS t = t_2$

Proof: By $\langle 9 \rangle 3$.

$\langle 9 \rangle 5$. $(\mathcal{E}_{N_1} \circledS t, \mathcal{E}_{N_2} \circledS t) \in \bigcup_{i=1}^{\#\psi} \psi[i]$

Proof: By $\langle 9 \rangle 4$ and $\langle 5 \rangle 1$.

$\langle 9 \rangle 6$. Q.E.D.

Proof: By $\langle 9 \rangle 2$, $\langle 9 \rangle 4$, $\langle 9 \rangle 5$ and the rule of replacement [51].

$\langle 8 \rangle 2$. Q.E.D.

Proof: $\subseteq$-rule.

$\langle 7 \rangle 3$. Q.E.D.

Proof: By $\langle 7 \rangle 1$, $\langle 7 \rangle 2$ and the =-rule for sets [29].

$\langle 6 \rangle 4$. $\bigcup_{i=1}^{\#\psi} \psi[i] \in \mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS \alpha)$

$\langle 7 \rangle 1$. $\mathcal{E}_{N_1} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \times \mathcal{E}_{N_2} \circledS \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS \alpha) \overline{\times} \mathcal{F}_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS \alpha)$

Proof: By $\langle 3 \rangle 1$ and Definition A.10.

$\langle 7 \rangle 2$. Q.E.D.

Proof: By $\langle 6 \rangle 3$, $\langle 7 \rangle 1$ and the rule of replacement.

$\langle 6 \rangle 5$. Q.E.D.

Proof: By $\langle 5 \rangle 2$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, $\langle 6 \rangle 4$ and $\Rightarrow$ elimination.

$\langle 5 \rangle 4$. $\forall i \in [1..\#\psi] : \{\Pi_1.p \mid p \in \psi[i]\} = \mathcal{E}_{N_1} \circledS \phi[i] \wedge \{\Pi_2.p \mid p \in \psi[i]\} = \mathcal{E}_{N_2} \circledS \phi[i]$

Proof: By $\langle 5 \rangle 1$.

$\langle 5 \rangle 5$. Q.E.D.

PROOF: By $\langle 5\rangle 3$, $\langle 5\rangle 4$ and the rule of replacement.

$\langle 4\rangle 3.$ Q.E.D.

PROOF: By assumption $\langle 2\rangle 1$, the cases $\langle 4\rangle 1$ and $\langle 4\rangle 2$ are exhaustive.

$\langle 3\rangle 5.$ $\sum_{i=1}^{\#\phi} f_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)(\mathcal{E}_{N_1} \circledS\, \phi[i]) \cdot f_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS\, \alpha)(\mathcal{E}_{N_2} \circledS\, \phi[i]) =$
$\sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi[i])$

$\langle 4\rangle 1.$ $\forall i \in [1..\#\phi] : \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi[i]) = f_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)(\mathcal{E}_{N_1} \circledS\, \phi[i]) \cdot f_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS\, \alpha)(\mathcal{E}_{N_2} \circledS\, \phi[i])$

PROOF: By definition (25) and $\langle 3\rangle 2$.

$\langle 4\rangle 2.$ Q.E.D.

PROOF: By $\langle 4\rangle 1$ and the rule of equality between functions [51].

$\langle 3\rangle 6.$ Q.E.D.

PROOF: By $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$ and the rule of transitivity [51].

$\langle 2\rangle 2.$ Q.E.D.

PROOF: By $\Rightarrow$-introduction.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: By $\forall$-introduction.

Lemma 5.6 *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$ and let $\mu_{N_1} \otimes \mu_{N_2}$ be a measure on the composite extended cone set of $D_{N_1} \otimes D_{N_2}$ as defined in (25). Then, for all complete queue histories $\alpha \in \mathcal{B}_{N_1 \cup N_2}$*

1. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\emptyset) = 0$
2. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ *is σ-additive*
3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

PROOF: (Proof of Lemma 5.6.1.)

$\langle 1\rangle 1.$ $\forall \alpha \in \mathcal{B}_N : \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\emptyset) = 0$

$\langle 2\rangle 1.$ ASSUME: $\alpha \in \mathcal{B}_N$
PROVE: $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\emptyset) = 0$

$\langle 3\rangle 1.$ $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\emptyset) = f_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)(\emptyset) \cdot f_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS\, \alpha)(\emptyset)$

$\langle 4\rangle 1.$ $\mathcal{E}_{N_1} \circledS\, \emptyset = \emptyset \wedge \mathcal{E}_{N_2} \circledS\, \emptyset = \emptyset$

PROOF: By definition (7).

$\langle 4\rangle 2.$ $\emptyset \in \mathcal{F}_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha) \wedge \emptyset \in \mathcal{F}_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS\, \alpha)$

PROOF: By assumption $\langle 2\rangle 1$, definition (21) and Definition 5.3.

$\langle 4\rangle 3.$ Q.E.D.

PROOF: By definition (25), $\langle 4\rangle 1$,$\langle 4\rangle 2$ and the rule of replacement.

$\langle 3\rangle 2.$ $f_{N_1}(\mathcal{E}_{N_1}^{\downarrow} \circledS\, \alpha)(\emptyset) = 0$

PROOF: By the assumption that I_{N_1} is a probabilistic component execution, Definition 5.3, Definition 5.1 and Definition A.6.

$\langle 3\rangle 3.$ $f_{N_2}(\mathcal{E}_{N_2}^{\downarrow} \circledS\, \alpha)(\emptyset) = 0$

PROOF: By the assumption that I_{N_2} is a probabilistic component execution, Definition 5.3, Definition 5.1 and Definition A.6.

$\langle 3\rangle 4.$ Q.E.D.

PROOF: By $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$ and elementary arithmetic.

$\langle 2\rangle 2.$ Q.E.D.

PROOF: $\forall$-introduction.

$\langle 1\rangle 2.$ Q.E.D.

PROOF. (Proof of Lemma 5.6.2.) Follows from Lemma B.28.

PROOF: (Proof of Lemma 5.6.3)

⟨1⟩1. $\forall \alpha \in \mathcal{B}_N : \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

⟨2⟩1. ASSUME: $\alpha \in \mathcal{B}_N$
PROVE: $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

⟨3⟩1. $\mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha)) \in \mathcal{F}_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \wedge \mathcal{E}_{N_2} \circledS (D_{N_1} \otimes D_{N_2}(\alpha)) \in \mathcal{F}_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)$

⟨4⟩1. $D_{N_1} \otimes D_{N_2}(\alpha) \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
PROOF: By Definition 3.3.

⟨4⟩2. Q.E.D.
PROOF: By ⟨4⟩1 and Theorem 5.5.

⟨3⟩2. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) = f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS D_{N_1} \otimes D_{N_2}(\alpha)) \cdot$
$f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS D_{N_1} \otimes D_{N_2}(\alpha))$
PROOF: By assumption ⟨2⟩1, ⟨3⟩1 and definition (25).

⟨3⟩3. $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS D_{N_1} \otimes D_{N_2}(\alpha)) \cdot$
$f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

⟨4⟩1. $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

⟨5⟩1. $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(\mathcal{E}_{N_1} \circledS D_{N_1} \otimes D_{N_2}(\alpha)) = f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1 - N_2}(\alpha))$

⟨6⟩1. $D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1 - N_2}(\alpha) = \mathcal{E}_{N_1} \circledS (D_{N_1} \otimes D_{N_2}(\alpha))$
PROOF: By Lemma B.25.

⟨6⟩2. Q.E.D.
PROOF: By ⟨6⟩1 and the rule of equality of functions [51].

⟨5⟩2. $D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha) \cap CT_{N_1 - N_2}(\alpha) \subseteq D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)$
PROOF: By definition (24).

⟨5⟩3. $f_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)(D_{N_1}(\mathcal{E}^{\downarrow}_{N_1} \circledS \alpha)) \leq 1$
PROOF: By the assumption that I_{N_1} is a probabilistic component execution, Definition 5.3, and Definition 5.1.

⟨5⟩4. Q.E.D.
PROOF: By ⟨5⟩1, ⟨5⟩2, ⟨5⟩3 and Lemma B.8.

⟨4⟩2. $f_{N_2}(\mathcal{E}^{\downarrow}_{N_2} \circledS \alpha)(\mathcal{E}_{N_2} \circledS D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$
PROOF: Symmetrical to ⟨4⟩1.

⟨4⟩3. Q.E.D.
PROOF: By ⟨4⟩1, ⟨4⟩2 and elementary arithmetic.

⟨3⟩4. Q.E.D.
PROOF: By ⟨3⟩2, ⟨3⟩3 and the rule of transitivity [51].

⟨2⟩2. Q.E.D.
PROOF: ∀-introduction.

⟨1⟩2. Q.E.D.

Lemma B.29. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$, let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Let $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ be a measure on $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as defined by (25) and let $F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ be an extension of $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as defined in Definition A.11. The function $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)$ defined* *by*

$$(33)\quad \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(c) \overset{\mathsf{def}}{=} \begin{cases} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(c) \ \textit{if}\ c \in C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \\ \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \\ \qquad\qquad\qquad \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha) \setminus c) \\ \textit{if}\ c \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \end{cases}$$

is a measure on $F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$.

PROOF:

⟨1⟩1. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\emptyset) = 0$

⟨2⟩1. $\emptyset \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By Definition A.11.

⟨2⟩2. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\emptyset) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By ⟨2⟩1 and definition (33)

⟨2⟩3. Q.E.D.

PROOF: By ⟨2⟩2.

⟨1⟩2. $\forall \phi \in \mathbb{P}(\mathcal{H})^{\omega} : \forall i \in [1..\#\phi] : \phi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\Rightarrow \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi[j])$

⟨2⟩1. ASSUME: $\phi \in \mathbb{P}(\mathcal{H})^{\omega}$
PROVE: $\forall i \in [1..\#\phi] : \phi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\Rightarrow \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi[j])$

⟨3⟩1. ASSUME: $\forall i \in [1..\#\phi] : \phi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
PROVE: $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi[j])$

⟨4⟩1. $\bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$

PROOF: By assumption ⟨3⟩1, Proposition B.1 ($F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \subseteq \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$) and elementary set theory.

⟨4⟩2. $\exists \phi' \in \mathbb{P}(\mathcal{H})^{\omega} : \forall i \in [1..\#\phi'] : \phi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge (\forall m, j \in [1..\#\phi'] : j \neq m \Rightarrow \phi'[j] \cap \phi'[m] = \emptyset) \wedge$
$\bigcup_{i=1}^{\#\phi'} \phi'[i] = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By ⟨4⟩1, Lemma B.14 and Corollary B.7.

⟨4⟩3. LET: $\phi' \in \mathbb{P}(\mathcal{H})^{\omega}$ such that $\forall i \in [1..\#\phi'] : \phi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge (\forall m, j \in [1..\#\phi'] : j \neq m \Rightarrow \phi'[j] \cap \phi'[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi'} \phi'[i] = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By ⟨4⟩2

⟨4⟩4. CASE: $\bigcup_{i=1}^{\#\phi'} \phi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

⟨5⟩1. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i])$

PROOF: By assumption ⟨4⟩4, ⟨4⟩3, the rule of replacement [51] and definition (33).

⟨5⟩2. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi'} \phi'[i])$

Proof: By ⟨4⟩3 and the rule of equality of functions [51].

⟨5⟩3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi'} \phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi[i])$

⟨6⟩1. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\bigcup_{i=1}^{\#\phi'} \phi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i])$

Proof: By ⟨4⟩3, assumption ⟨4⟩4 and Lemma B.28.

⟨6⟩2. $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi'[i])$

⟨7⟩1. $\forall i \in [1..\#\phi'] : \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i]) = \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi'[i])$

Proof: By ⟨4⟩3 and definition (33).

⟨7⟩2. Q.E.D.

Proof: By ⟨7⟩1 and the rule of equality between functions.

⟨6⟩3. $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi[i])$

Proof: By ⟨4⟩3 and definition (33), since ϕ and ϕ' are two different partitions of the same set.

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩1, ⟨6⟩2 ⟨6⟩3 and the rule of transitivity [51].

⟨5⟩4. Q.E.D.

Proof: By ⟨5⟩1, ⟨5⟩2, ⟨5⟩3 and the rule of transitivity [51].

⟨4⟩5. Case: $\bigcup_{i=1}^{\#\phi'} \phi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

⟨5⟩1. $D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi'} \phi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

Proof: By assumption ⟨4⟩5 and Definition A.11.

⟨5⟩2. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) =$
$\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i])$

Proof: By assumption ⟨4⟩5, ⟨4⟩3, the rule of replacement [51] and definition (33).

⟨5⟩3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i]) =$
$\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i])$

⟨6⟩1. Let: $\psi' = \langle D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i] \rangle \frown \phi'$

⟨6⟩2. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) = \sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$

⟨7⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] = D_{N_1} \otimes D_{N_2}(\alpha)$

⟨8⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] = \bigcup_{i=1}^{\#\phi'} \phi'[i] \cup D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i]$

Proof: By ⟨6⟩1.

⟨8⟩2. $\bigcup_{i=1}^{\#\phi'} \phi'[i] \cup (D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i]) = D_{N_1} \otimes D_{N_2}(\alpha)$

⟨9⟩1. $\bigcup_{i=1}^{\#\phi} \phi[i] \cup (D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i]) = D_{N_1} \otimes D_{N_2}(\alpha)$

⟨10⟩1. $\bigcup_{i=1}^{\#\phi} \phi[i] \subseteq D_{N_1} \otimes D_{N_2}(\alpha)$

⟨11⟩1. $\forall A \in \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha) : A \subseteq D_{N_1} \otimes D_{N_2}(\alpha)$

Proof: By Definition A.4 and Definition A.3.

⟨11⟩2. Q.E.D.

Proof: By assumption ⟨3⟩1, Proposition B.1 ($F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \subseteq \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$), ⟨11⟩1 and $\forall$ elimination.

⟨10⟩2. Q.E.D.

Proof: By ⟨10⟩1 and elementary set theory.

⟨9⟩2. Q.E.D.

Proof: By ⟨9⟩1 and⟨4⟩3.

⟨8⟩3. Q.E.D.
Proof: By ⟨8⟩1, ⟨8⟩2 and the rule of transitivity [51].

⟨7⟩2. $\forall i \in [1..\#\psi'] : \psi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge (\forall m, j \in [1..\#\psi'] : j \neq m \Rightarrow \psi'[j] \cap \psi'[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\psi'} \psi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

⟨8⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
Proof: By ⟨7⟩1 and Definition 3.3.

⟨8⟩2. $\forall i \in [1..\#\psi'] : \psi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
Proof: By ⟨5⟩1, ⟨4⟩3 and ⟨6⟩1.

⟨8⟩3. $\forall m, j \in [1..\#\psi'] : j \neq m \Rightarrow \psi'[j] \cap \psi'[m] = \emptyset$
Proof: By ⟨4⟩3 and ⟨6⟩1.

⟨8⟩4. Q.E.D.
Proof: By ⟨8⟩1, ⟨8⟩2, ⟨8⟩3 and ∧-introduction.

⟨7⟩3. Q.E.D.
Proof: By ⟨7⟩1, ⟨7⟩2 and Lemma 5.6.

⟨6⟩3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i]) =$
$\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i]) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1])$

⟨7⟩1. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi} \phi[i]) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1])$
Proof: By ⟨6⟩1 and the rule of equality between functions [51].

⟨7⟩2. Q.E.D.
Proof: By ⟨7⟩1, ⟨6⟩2 and the rule of replacement [51].

⟨6⟩4. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i]) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1]) =$
$\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i])$

⟨7⟩1. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i]) - \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1]) =$
$\sum_{i=2}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$

⟨8⟩1. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i]) \leq 1$

⟨9⟩1. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$.
Proof: By the assumption that $\mu_{N_1} \otimes \mu_{N_2}$ is a measure on $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as defined by (25) and Lemma 5.6.3.

⟨9⟩2. Q.E.D.
Proof: By ⟨6⟩2, ⟨9⟩1 and the rule of replacement [51].

⟨8⟩2. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) =$
$\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1]) + \sum_{i=2}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$
Proof: By ⟨6⟩1, ⟨6⟩2 and ⟨8⟩1, since the sum of the terms of a converging series is preserved when regrouping the terms in the same order [50].

⟨8⟩3. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i]) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1]) +$
$\sum_{i=2}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$
Proof: By ⟨8⟩2, ⟨6⟩2 and the rule of transitivity [51].

⟨8⟩4. Q.E.D.
Proof: By ⟨8⟩3 and elementary arithmetic. The possibility to apply the rules of elementary arithmetic follows from the fact that $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$ converges to a finite number, by ⟨8⟩1 and that $\mu_{N_1} \otimes$

$\mu_{N_2}(\alpha)(\psi'[1])$ and $\sum_{i=2}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$ also converges to finite numbers by $\langle 8\rangle 3$.

$\langle 7\rangle 2.$ $\sum_{i=2}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i])$
Proof: By $\langle 6\rangle 1$

$\langle 7\rangle 3.$ Q.E.D.
Proof: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and the rule of transitivity [51].

$\langle 6\rangle 5.$ Q.E.D.
Proof: By $\langle 6\rangle 3$, $\langle 6\rangle 4$ and the rule of transitivity [51].

$\langle 5\rangle 4.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi[i])$

$\langle 6\rangle 1.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi'[i])$

$\langle 7\rangle 1.$ $\forall i \in [1..\#\phi'] : \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\phi'[i]) = \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi'[i])$
Proof: By $\langle 4\rangle 3$ and definition (33).

$\langle 7\rangle 2.$ Q.E.D.
Proof: By $\langle 7\rangle 1$ and the rule of equality between functions.

$\langle 6\rangle 2.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi[i])$
Proof: By $\langle 4\rangle 3$, since ϕ' and ϕ are two different partitions of the same set.

$\langle 6\rangle 3.$ Q.E.D.
Proof: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and the rule of transitivity [51].

$\langle 5\rangle 5.$ Q.E.D.
Proof: By $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$ and the rule of transitivity.

$\langle 4\rangle 6.$ Q.E.D.
Proof: By assumption $\langle 3\rangle 1$ and Definition A.11, the cases $\langle 4\rangle 4$ and $\langle 4\rangle 5$ are exhaustive.

$\langle 3\rangle 2.$ Q.E.D.
Proof: $\Rightarrow$-introduction.

$\langle 2\rangle 2.$ Q.E.D.
Proof: $\forall$-introduction.

$\langle 1\rangle 3.$ Q.E.D.
Proof: By $\langle 1\rangle 1$, $\langle 1\rangle 2$ and Definition A.6.

Lemma B.30. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Let $F_1(C_E(D_N(\alpha)))$ be an extension of $C_E(D_N(\alpha))$ as defined in Definition A.11. Then*

$$\forall B, A \in F_1(C_E(D_N(\alpha))) : (B \cap A \neq \emptyset) \Rightarrow (((D_N(\alpha) \setminus B) \cap (D_N(\alpha) \setminus A) = \emptyset) \vee \\ (((D_N(\alpha) \setminus B) \subseteq (D_N(\alpha) \setminus A)) \vee ((D_N(\alpha) \setminus A) \subseteq (D_N(\alpha) \setminus B))))$$

Proof:

$\langle 1\rangle 1.$ Assume: $A \in F_1(C_E(D_N(\alpha))) \wedge B \in F_1(C_E(D_N(\alpha)))$
Prove: $(B \cap A \neq \emptyset) \Rightarrow (((D_N(\alpha) \setminus B) \cap (D_N(\alpha) \setminus A) = \emptyset) \vee$
$(((D_N(\alpha) \setminus B) \subseteq (D_N(\alpha) \setminus A)) \vee ((D_N(\alpha) \setminus A) \subseteq (D_N(\alpha) \setminus B))))$

$\langle 2\rangle 1.$ Assume: $B \cap A \neq \emptyset$
Prove: $((D_N(\alpha) \setminus B) \cap (D_N(\alpha) \setminus A) = \emptyset) \vee (((D_N(\alpha) \setminus B) \subseteq (D_N(\alpha) \setminus A)) \vee$
$((D_N(\alpha) \setminus A) \subseteq (D_N(\alpha) \setminus B)))$

$\langle 3\rangle 1.$ Case: $A \in C_E(D_N(\alpha)) \wedge B \in C_E(D_N(\alpha))$

$\langle 4\rangle 1.$ $A \subseteq B \vee B \subseteq A$

PROOF: By assumption $\langle 3\rangle 1$ and Corollary B.6.

$\langle 4\rangle 2.$ $(((D_N(\alpha) \setminus B) \subseteq (D_N(\alpha) \setminus A)) \vee ((D_N(\alpha) \setminus A) \subseteq (D_N(\alpha) \setminus B)))$

PROOF: By $\langle 4\rangle 1$ and elementary set theory.

$\langle 4\rangle 3.$ Q.E.D.

PROOF: By $\langle 4\rangle 2$ and $\vee$ introduction.

$\langle 3\rangle 2.$ CASE: $(D_N(\alpha) \setminus A) \in C_E(D_N(\alpha)) \wedge (D_N(\alpha) \setminus B) \in C_E(D_N(\alpha))$

$\langle 4\rangle 1.$ Q.E.D.

PROOF: By assumption $\langle 3\rangle 2$ and Corollary B.6.

$\langle 3\rangle 3.$ CASE: $(D_N(\alpha) \setminus A) \in C_E(D_N(\alpha)) \wedge B \in C_E(D_N(\alpha))$

$\langle 4\rangle 1.$ $B \not\subseteq (D_N(\alpha) \setminus A)$

PROOF: By assumption $\langle 2\rangle 1$ and elementary set theory.

$\langle 4\rangle 2.$ CASE: $(D_N(\alpha) \setminus A) \subseteq B$

$\langle 5\rangle 1.$ $(D_N(\alpha) \setminus A) \cap (D_N(\alpha) \setminus B) = \emptyset$

PROOF: By assumption $\langle 4\rangle 2$ and elementary set theory.

$\langle 5\rangle 2.$ Q.E.D.

PROOF: By $\langle 5\rangle 1$ and $\vee$ introduction.

$\langle 4\rangle 3.$ CASE: $(D_N(\alpha) \setminus A) \cap B = \emptyset$

$\langle 5\rangle 1.$ $(D_N(\alpha) \setminus A) \subseteq (D_N(\alpha) \setminus B)$

PROOF: By assumption $\langle 4\rangle 3$ and elementary set theory.

$\langle 5\rangle 2.$ Q.E.D.

PROOF: By $\langle 5\rangle 1$ and $\vee$ introduction.

$\langle 4\rangle 4.$ Q.E.D.

PROOF: By $\langle 4\rangle 1$, the cases $\langle 4\rangle 2$ and $\langle 4\rangle 3$ are exhaustive.

$\langle 3\rangle 4.$ CASE: $A \in C_E(D_N(\alpha)) \wedge (D_N(\alpha) \setminus B) \in C_E(D_N(\alpha))$

PROOF: Symmetrical to step $\langle 3\rangle 3$.

$\langle 3\rangle 5.$ Q.E.D.

PROOF: By assumption $\langle 1\rangle 1$, the cases $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$ and $\langle 3\rangle 4$ are exhaustive.

$\langle 2\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$ introduction.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\forall$ introduction.

Corollary B.31. *Let I_N be a probabilistic component execution as defined in Definition 5.3 and let α be a complete queue history $\alpha \in \mathcal{B}_N$. Let $F_1(C_E(D_N(\alpha)))$ be an extension of $C_E(D_N(\alpha))$ as defined in Definition A.11. Let $\bigcap_i^n A_i$ be a non-empty intersection of finitely many elements such that $\forall i \in [1..n] : A_i \in F_1(C)$. Then there is a finite sequence ψ of disjoint elements in $F_1(C)$ such that*

$$\#\psi \leq n \wedge \bigcup_{i=1}^{\#\psi} \psi[i] = D_N(\alpha) \setminus \bigcap_{i=1}^{n} A_i$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $A_1 \in F_1(C_E(D_N(\alpha))) \wedge \cdots \wedge A_n \in F_1(C_E(D_N(\alpha))) \wedge \bigcap_i^n A_i \neq \emptyset$

PROVE: $\exists \psi \in \mathbb{P}(\mathcal{H}_N)^* : \forall i \in [1..\#\psi] : \psi[i] \in F_1(C_E(D_N(\alpha)))$
$\wedge (\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset) \wedge \#\psi \leq n$
$\wedge \bigcup_{i=1}^{\#\psi} \psi[i] = D_N(\alpha) \setminus \bigcap_{i=1}^{n} A_i$

$\langle 2\rangle 1.$ LET: ψ' be a sequence in $\mathbb{P}(\mathcal{H}_N)^n$ such that $\forall i \in [1..n] : \psi'[i] = D_N(\alpha) \setminus A_i$.

$\langle 2 \rangle 2.$ $\forall i \in [1..n] : \psi'[i] \in F_1(C_E(D_N(\alpha)))$
PROOF: By assumption $\langle 1 \rangle 1$, $\langle 2 \rangle 1$ and Definition A.11.

$\langle 2 \rangle 3.$ $\forall j, m \in [1..n] : j \neq m \Rightarrow$
$((\psi'[j] \cap \psi'[m] = \emptyset) \vee ((\psi'[j] \subseteq \psi'[m]) \vee (\psi'[m] \subseteq \psi'[j])))$
PROOF: By assumption $\langle 1 \rangle 1$, $\langle 2 \rangle 1$ and Lemma B.30.

$\langle 2 \rangle 4.$ $\exists \psi \in \mathbb{P}(\mathcal{H}_N)^* : \forall i \in [1..\#\psi] : \psi[i] \in F_1(C_E(D_N(\alpha))) \wedge$
$\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset \wedge \#\psi \leq \#\psi' \wedge \bigcup_{i=1}^{\#\psi} \psi[i] = \bigcup_{j=1}^{\#\psi'} \psi'[j]$
PROOF: By $\langle 2 \rangle 2$ and $\langle 2 \rangle 3$ (let ψ be the sequence obtained from ψ' by filtering away all elements $\psi'[j]$ such that $j \in [1..\#\psi'] \wedge \exists i \in [1..\#\psi'] : i \neq j \wedge \psi'[j] \subseteq \psi'[i]$).

$\langle 2 \rangle 5.$ LET: $\psi \in \mathbb{P}(\mathcal{H}_N)^*$ such that $\forall i \in [1..\#\psi] : \psi[i] \in F_1(C_E(D_N(\alpha))) \wedge$
$\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset \wedge \#\psi \leq \#\psi' \wedge$
$\bigcup_{i=1}^{\#\psi} \psi[i] = \bigcup_{j=1}^{\#\psi'} \psi'[j]$
PROOF: By $\langle 2 \rangle 4$.

$\langle 2 \rangle 6.$ $\#\psi \leq n$

$\langle 3 \rangle 1.$ $\#\psi' = n$
PROOF: By $\langle 2 \rangle 1$.

$\langle 3 \rangle 2.$ Q.E.D.
PROOF: By $\langle 3 \rangle 1$, $\langle 2 \rangle 5$ ($\#\psi \leq \#\psi'$) and the rule of replacement.

$\langle 2 \rangle 7.$ $\bigcup_{i=1}^{\#\psi} \psi[i] = D_N(\alpha) \setminus \bigcup_{i=1}^{n} A_i$

$\langle 3 \rangle 1.$ $\bigcup_{i=1}^{\#\psi} \psi'[i] = \bigcup_{i=1}^{n} (D_N(\alpha) \setminus A_i)$
PROOF: By $\langle 2 \rangle 1$.

$\langle 3 \rangle 2.$ $\bigcup_{i=1}^{n} (D_N(\alpha) \setminus A_i) = D_N(\alpha) \setminus \bigcap_{i=1}^{n} A_i$
PROOF: By elementary set theory.

$\langle 3 \rangle 3.$ Q.E.D.
PROOF: By $\langle 2 \rangle 5$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$ and the rule of transitivity [51].

$\langle 2 \rangle 8.$ Q.E.D.
PROOF: By $\langle 2 \rangle 5$, $\langle 2 \rangle 6$ $\langle 2 \rangle 7$ and $\exists$ introduction.

$\langle 1 \rangle 2.$ Q.E.D.
PROOF: $\Rightarrow$ introduction.

Lemma B.32. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$, let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Let $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)$ be a measure on $F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ as defined in (33) and let $F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ be an extension of $F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ as defined in Definition A.11. The function $\mu_{N_1} \otimes {\mu_{N_2}}''(\alpha)$ defined by*

$$(34) \quad \mu_{N_1} \otimes {\mu_{N_2}}''(\alpha)(A) \overset{\mathsf{def}}{=}$$
$$\begin{cases} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(A) \textit{ if } A \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \\ \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \sum_{j=1}^{m} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi[j]) \\ \textit{if } A \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \\ \textsf{where } B_1, \ldots B_n \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \wedge \psi \in (F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))))^* \\ \textsf{so that } \; A = \bigcap_{i=1}^{n} B_i \wedge \forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset \wedge \\ \qquad \bigcup_{j=1}^{m} \psi[j] = D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcap_{i=1}^{n} B_i \text{[9]} \end{cases}$$

is a measure on $F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$.

PROOF:

$\langle 1\rangle 1.$ $\mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\emptyset) = 0$

$\langle 2\rangle 1.$ $\emptyset \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

PROOF: By Definition B.1.

$\langle 2\rangle 2.$ $\mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\emptyset) = \mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\emptyset)$

PROOF: By $\langle 2\rangle 1$ and definition (34).

$\langle 2\rangle 3.$ $\mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\emptyset) = 0$

PROOF: By Lemma B.29.

$\langle 2\rangle 4.$ Q.E.D.

PROOF: By $\langle 2\rangle 2$, $\langle 2\rangle 3$ and the rule of transitivity.

$\langle 1\rangle 2.$ $\forall \phi \in \mathbb{P}(\mathcal{H})^{\,\omega} : (\forall i \in [1..\#\phi] : \phi[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))))$
$\Rightarrow \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi[j])$

$\langle 2\rangle 1.$ ASSUME: $\phi \in \mathbb{P}(\mathcal{H})^{\,\omega}$
PROVE: $(\forall i \in [1..\#\phi] : \phi[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))))$
$\Rightarrow \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi[j])$

$\langle 3\rangle 1.$ ASSUME: $\forall i \in [1..\#\phi] : \phi[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi} \phi[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
PROVE: $\mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi[j])$

$\langle 4\rangle 1.$ $\bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$

PROOF: By assumption $\langle 3\rangle 1$, Proposition B.1 ($F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \subseteq \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$) and elementary set theory.

$\langle 4\rangle 2.$ $\exists \phi' \in \mathbb{P}(\mathcal{H})^{\,\omega} : \forall i \in [1..\#\phi'] : \phi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge\, (\forall m, j \in [1..\#\phi'] : j \neq m \Rightarrow \phi'[j] \cap \phi'[m] = \emptyset) \,\wedge$
$\bigcup_{i=1}^{\#\phi'} \phi'[i] = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By $\langle 4\rangle 1$, Lemma B.14 and Corollary B.7.

$\langle 4\rangle 3.$ LET: $\phi' \in \mathbb{P}(\mathcal{H})^{\,\omega}$ such that $\forall i \in [1..\#\phi'] : \phi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$
$\wedge\, (\forall m, j \in [1..\#\phi'] : j \neq m \Rightarrow \phi'[j] \cap \phi'[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\phi'} \phi'[i] = \bigcup_{i=1}^{\#\phi} \phi[i]$

PROOF: By $\langle 4\rangle 2$

$\langle 4\rangle 4.$ CASE: $\bigcup_{i=1}^{\#\phi'} \phi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

$\langle 5\rangle 1.$ $\mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i])$

PROOF: By assumption $\langle 4\rangle 4$, $\langle 4\rangle 3$, the rule of replacement [51] and definition (34).

$\langle 5\rangle 2.$ $\mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\bigcup_{i=1}^{\#\phi'} \phi'[i])$

[9] Note that by Definition A.11, if $A \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$, then A corresponds to the intersection of finitely many elements in $F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$. Note also that there may exist several sequences ψ of disjoint elements in $F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ such that $\bigcup_{j=1}^{m} \psi[j] = D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcap_{i=1}^{n} B_i$. However, since $\mu_{N_1} \otimes \mu_{N_2}'(\alpha)$ is a measure, by Lemma B.29, the sum of the measures of their elements will all be the same.

Proof: By $\langle 4\rangle 3$ and the rule of equality of functions [51].

$\langle 5\rangle 3.$ $\mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\bigcup_{i=1}^{\#\phi'} \phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}{}''(\alpha)(\phi[i])$

$\langle 6\rangle 1.$ $\mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\bigcup_{i=1}^{\#\phi'} \phi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi'[i])$

Proof: By $\langle 4\rangle 3$, assumption $\langle 4\rangle 4$ and Lemma B.29.

$\langle 6\rangle 2.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)'(\phi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}{}''(\alpha)(\phi'[i])$

$\langle 7\rangle 1.$ $\forall i \in [1..\#\phi'] : \mu_{N_1} \otimes \mu_{N_2}{}''(\alpha)(\phi'[i]) = \mu_{N_1} \otimes \mu'_{N_2}(\alpha)(\phi'[i])$

$\langle 8\rangle 1.$ $\forall i \in [1..\#\phi'] : \phi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

Proof: By $\langle 4\rangle 3$ and Definition A.11.

$\langle 8\rangle 2.$ Q.E.D.

Proof: By $\langle 8\rangle 1$ and definition (34).

$\langle 7\rangle 2.$ Q.E.D.

Proof: By $\langle 7\rangle 1$ and the rule of equality between functions.

$\langle 6\rangle 3.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}{}''(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}{}''(\alpha)(\phi[i])$

Proof: By definition (34), $\langle 4\rangle 3$, since ϕ and ϕ' are two different partitions of the same set.

$\langle 6\rangle 4.$ Q.E.D.

Proof: By $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$ and the rule of transitivity [51].

$\langle 5\rangle 4.$ Q.E.D.

Proof: By $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ and the rule of transitivity [51].

$\langle 4\rangle 5.$ Case: $\bigcup_{i=1}^{\#\phi'} \phi'[i] \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

$\langle 5\rangle 1.$ $\exists A_1, \ldots A_n \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) : \bigcup_{i=1}^{\#\phi'} \phi'[i] = \bigcap_{i=1}^{n} A_i$

Proof: By assumption $\langle 4\rangle 5$ and Definition A.11.

$\langle 5\rangle 2.$ Let: $A_1, \ldots A_n \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ such that $\bigcup_{i=1}^{\#\phi'} \phi'[i] = \bigcap_{i=1}^{n} A_i$

Proof: By $\langle 5\rangle 1$.

$\langle 5\rangle 3.$ $\bigcap_{i=1}^{n} A_i \neq \emptyset$

Proof: By assumption $\langle 4\rangle 5$ and Definition A.11.

$\langle 5\rangle 4.$ $\exists \psi \in \mathbb{P}(\mathcal{H})^* : \forall i \in [1..\#\psi] : \psi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge (\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset) \wedge \#\psi \leq n$
$\wedge \bigcup_{i=1}^{\#\psi} \psi[i] = D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcap_{i=1}^{n} A_i$

Proof: By $\langle 5\rangle 2$, $\langle 5\rangle 3$ and Corollary B.31.

$\langle 5\rangle 5.$ Let: $\psi \in \mathbb{P}(\mathcal{H})^*$ such that $\forall i \in [1..\#\psi] : \psi[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge (\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi[j] \cap \psi[m] = \emptyset) \wedge \#\psi \leq n$
$\wedge \bigcup_{i=1}^{\#\psi} \psi[i] = D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcap_{i=1}^{n} A_i$

Proof: By $\langle 5\rangle 4$.

$\langle 5\rangle 6.$ $\mu_{N_1} \otimes \mu_{N_2}{}''(\alpha)(\bigcup_{i=1}^{\#\phi} \phi[i]) = \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) -$
$\sum_{j=1}^{\#\psi} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\psi[j])$

Proof: By assumption $\langle 4\rangle 5$, $\langle 5\rangle 5$, $\langle 4\rangle 3$, the rule of replacement [51] and definition (33).

$\langle 5\rangle 7.$ $\mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \sum_{j=1}^{\#\psi} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\psi[j]) =$
$\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(\phi'[i])$

$\langle 6\rangle 1.$ Let: $\psi' = \psi \frown \phi'$

$\langle 6\rangle 2.$ $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)'(\psi'[i]) = \mu_{N_1} \otimes \mu_{N_2}{}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 7\rangle 1.$ $\bigcup_{i=1}^{\#\psi} \psi'[i] = D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi'} \phi'[i]$

$\langle 8\rangle 1.$ $\bigcup_{i=1}^{\#\psi} \psi'[i] = \bigcup_{i=1}^{\#\psi} \psi[i]$

PROOF: By ⟨6⟩1.

⟨8⟩2. $\bigcup_{i=1}^{\#\psi} \psi[i] = D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi'} \phi'[i]$

PROOF: By ⟨5⟩2, ⟨5⟩5 and the rule of replacement [51].

⟨8⟩3. Q.E.D.

PROOF: By ⟨8⟩1, ⟨8⟩2 and the rule of replacement [51].

⟨7⟩2. $\bigcup_{j=\#\psi+1}^{\#\psi'} \psi'[j] = \bigcup_{i=1}^{\#\phi'} \phi'[i]$

PROOF: By ⟨6⟩1.

⟨7⟩3. $\bigcup_{i=1}^{\#\psi'} \psi'[i] = D_{N_1} \otimes D_{N_2}(\alpha)$

⟨8⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] = (D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi'} \phi'[i]) \cup \bigcup_{i=1}^{\#\phi'} \phi'[i]$

⟨9⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] = (\bigcup_{i=1}^{\#\psi} \psi'[i]) \cup (\bigcup_{j=\#\psi+1}^{\#\psi'} \psi'[j])$

PROOF: By ⟨5⟩5 and ⟨6⟩1.

⟨9⟩2. Q.E.D.

PROOF: By ⟨9⟩1, ⟨7⟩1, ⟨7⟩2 and the rule of replacement [51].

⟨8⟩2. $(D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi'} \phi'[i]) \cup \bigcup_{i=1}^{\#\phi'} \phi'[i] = D_{N_1} \otimes D_{N_2}(\alpha)$

PROOF: By elementary set theory.

⟨8⟩3. Q.E.D.

PROOF: By ⟨8⟩1, ⟨8⟩2 and the rule of transitivity.

⟨7⟩4. $\forall i \in [1..\#\psi'] : \psi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$
$\wedge (\forall m, j \in [1..\#\psi'] : j \neq m \Rightarrow \psi'[j] \cap \psi'[m] = \emptyset)$
$\wedge \bigcup_{i=1}^{\#\psi'} \psi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

⟨8⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

⟨9⟩1. $\bigcup_{i=1}^{\#\psi'} \psi'[i] \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By ⟨7⟩3, Definition 3.3 and the fact that $c(\langle\rangle, D_{N_1} \otimes D_{N_2}(\alpha)) = D_{N_1} \otimes D_{N_2}(\alpha)$, by Definition 3.1.

⟨9⟩2. Q.E.D.

PROOF: By ⟨9⟩1, Proposition B.1 ($C_E(D_{N_1} \otimes D_{N_2}(\alpha)) \subseteq F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$) and elementary set theory.

⟨8⟩2. $\forall i \in [1..\#\psi'] : \psi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

⟨9⟩1. $\forall i \in [1..\#\phi'] : \phi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

PROOF: By ⟨4⟩3 and Definition A.11.

⟨9⟩2. Q.E.D.

PROOF: By ⟨5⟩5, ⟨9⟩1 and ⟨6⟩1.

⟨8⟩3. $\forall m, j \in [1..\#\psi'] : j \neq m \Rightarrow \psi'[j] \cap \psi'[m] = \emptyset$

⟨9⟩1. $\forall m, j \in [1..\#\psi] : j \neq m \Rightarrow \psi'[j] \cap \psi'[m] = \emptyset$

PROOF: By ⟨5⟩5 and and ⟨6⟩1.

⟨9⟩2. $\forall m, j \in [\#\psi + 1..\#\psi'] : j \neq m \Rightarrow \psi'[j] \cap \psi'[m] = \emptyset$

PROOF: By ⟨4⟩3 and and ⟨6⟩1.

⟨9⟩3. $(\bigcup_{i=1}^{\#\psi} \psi'[i]) \cap (\bigcup_{j=\#\psi+1}^{\#\psi'} \psi'[j]) = \emptyset$

⟨10⟩1. $(D_{N_1} \otimes D_{N_2}(\alpha) \setminus \bigcup_{i=1}^{\#\phi'} \phi'[i]) \cap \bigcup_{i=1}^{\#\phi'} \phi'[i] = \emptyset$

PROOF: By elementary set theory.

PROOF: By ⟨10⟩1, ⟨7⟩1, ⟨7⟩2 and the rule of replacement [51].

⟨9⟩4. Q.E.D.

PROOF: By ⟨9⟩1, ⟨9⟩2, ⟨9⟩3 and elementary set theory.

⟨8⟩4. Q.E.D.

PROOF: By ⟨8⟩1, ⟨8⟩2, ⟨8⟩3 and $\wedge$ -introduction.

⟨7⟩5. Q.E.D.

PROOF: By ⟨7⟩3, ⟨7⟩4 and Lemma B.29.

⟨6⟩3. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) - \sum_{j=1}^{\#\psi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi[j]) =$
$\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) - \sum_{i=1}^{\#\psi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i])$

PROOF: By ⟨6⟩1 and ⟨6⟩2.

⟨6⟩4. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) - \sum_{i=1}^{\#\psi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) =$
$\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi'[i])$

⟨7⟩1. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) - \sum_{i=1}^{\#\psi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) =$
$\sum_{i=\#\psi+1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i])$

⟨8⟩1. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) \leq 1$

⟨9⟩1. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$.

⟨10⟩1. $D_{N_1} \otimes D_{N_2}(\alpha) \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By the fact that $c(\langle\rangle, D_{N_1} \otimes D_{N_2}(\alpha)) = D_{N_1} \otimes D_{N_2}(\alpha)$, by Definition 3.1.

⟨10⟩2. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By ⟨10⟩1 and Lemma B.29.

⟨10⟩3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$.

PROOF: By definition (25) and Lemma 5.6.3.

⟨10⟩4. Q.E.D.

PROOF: By ⟨10⟩2, ⟨10⟩3 and the rule of replacement [51].

⟨9⟩2. Q.E.D.

PROOF: By ⟨6⟩2, ⟨9⟩1 and the rule of replacement [51].

⟨8⟩2. $\mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) =$
$\sum_{i=1}^{\#\psi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) + \sum_{i=\#\psi+1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i])$

PROOF: By ⟨6⟩1, ⟨6⟩2 and ⟨8⟩1, since the sum of the terms of a converging series is preserved when regrouping the terms in the same order [50].

⟨8⟩3. $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) =$
$\sum_{i=1}^{\#\psi} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) + \sum_{i=\#\psi+1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i])$

PROOF: By ⟨8⟩2, ⟨6⟩2 and the rule of transitivity [51].

⟨8⟩4. Q.E.D.

PROOF: By ⟨8⟩3 and elementary arithmetic. The possibility to apply the rules of elementary arithmetic follows from the fact that $\sum_{i=1}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$ converges to a finite number, by ⟨8⟩1 and that $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[1])$ and $\sum_{i=2}^{\#\psi'} \mu_{N_1} \otimes \mu_{N_2}(\alpha)(\psi'[i])$ also converges to finite numbers by ⟨8⟩3.

⟨7⟩2. $\sum_{i=\#\psi+1}^{\#\psi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\psi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes {\mu_{N_2}}'(\alpha)(\phi'[i])$

PROOF: By ⟨6⟩1

⟨7⟩3. Q.E.D.

PROOF: By ⟨7⟩1, ⟨7⟩2 and the rule of transitivity [51].

⟨6⟩5. Q.E.D.

PROOF: By ⟨6⟩3, ⟨6⟩4 and the rule of transitivity [51].

$\langle 5\rangle 8.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi[i])$

$\langle 6\rangle 1.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi'[i])$

$\langle 7\rangle 1.$ $\forall i \in [1..\#\phi'] : \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi'[i]) = \mu_{N_1} \otimes \mu_{N_2}'(\alpha)(\phi'[i])$

$\langle 8\rangle 1.$ $\forall i \in [1..\#\phi'] : \phi'[i] \in F_1(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

Proof: By $\langle 4\rangle 3$ and Definition A.11.

$\langle 8\rangle 2.$ Q.E.D.

Proof: By $\langle 8\rangle 1$ and definition (34).

$\langle 7\rangle 2.$ Q.E.D.

Proof: By $\langle 7\rangle 1$ and the rule of equality between functions.

$\langle 6\rangle 2.$ $\sum_{i=1}^{\#\phi'} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi'[i]) = \sum_{i=1}^{\#\phi} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\phi[i])$

Proof: By definition (34) and $\langle 4\rangle 3$, since ϕ' and ϕ are two different partitions of the same set.

$\langle 6\rangle 3.$ Q.E.D.

Proof: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and the rule of transitivity [51].

$\langle 5\rangle 9.$ Q.E.D.

Proof: By $\langle 5\rangle 6$, $\langle 5\rangle 7$, $\langle 5\rangle 8$ and the rule of transitivity.

$\langle 4\rangle 6.$ Q.E.D.

Proof: By assumption $\langle 3\rangle 1$, the cases $\langle 4\rangle 4$ and $\langle 4\rangle 5$ are exhaustive.

$\langle 3\rangle 2.$ Q.E.D.

Proof: $\Rightarrow$-introduction.

$\langle 2\rangle 2.$ Q.E.D.

Proof: $\forall$-introduction.

$\langle 1\rangle 3.$ Q.E.D.

Proof: By $\langle 1\rangle 1$, $\langle 1\rangle 2$ and Definition A.6..

Lemma B.33. *Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$, let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$. Let $\mu_{N_1} \otimes \mu_{N_2}''(\alpha)$ be a measure on $F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ as defined in Lemma B.32 and let $F_3(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ be an extension of $F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$ as defined in Definition A.11. The function $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)$ defined by*

$$(35) \quad \mu_{N_1} \otimes \mu_{N_2}'''(\alpha)(A) \overset{\mathsf{def}}{=} \begin{cases} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(A) \text{ if } A \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \\ \sum_{i=1}^{n} \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(B_i) \text{ if } A \in \\ F_3(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \\ \textsf{where } B_1, \ldots B_n \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \\ \textsf{so that } A = \bigcup_{i=1}^{n} B_i{}^{10} \end{cases}$$

is a measure on $F_3(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$.

Proof:

$\langle 1\rangle 1.$ $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)(\emptyset) = 0$

$\langle 2\rangle 1.$ $\emptyset \in F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

[10] Note that by Definition A.11, if $A \in F_3(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) \setminus F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$, then A corresponds to the union of finitely many elements in $F_2(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$.

PROOF: By Definition A.11 and Proposition B.1.

⟨2⟩2. $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)(\emptyset) = \mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\emptyset)$

PROOF: By ⟨2⟩1 and definition (35).

⟨2⟩3. $\mu_{N_1} \otimes \mu_{N_2}''(\alpha)(\emptyset) = 0$

PROOF: By Lemma B.32.

⟨2⟩4. Q.E.D.

PROOF: By ⟨2⟩2, ⟨2⟩3 and the rule of transitivity.

⟨1⟩2. $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)$ is σ-additive.

PROOF: By definition (35) and Lemma B.32.

⟨1⟩3. Q.E.D.

PROOF: By ⟨1⟩1, ⟨1⟩2 and Definition A.6..

Theorem 5.7*Let I_{N_1} and I_{N_2} be two probabilistic component executions such that $N_1 \cap N_2 = \emptyset$, let α be a queue history in $\mathcal{B}_{N_1 \cup N_2}$, and let $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ be a measure on $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$ as defined in (25). Then, there exists a unique extension $f_{N_1} \otimes f_{N_2}(\alpha)$ of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to the cone-σ-field $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.*

PROOF:

⟨1⟩1. There exists a unique extension of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to the cone-σ-field $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$

⟨2⟩1. There exists a unique extension $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)$ of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to $F(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

⟨3⟩1. There exists a unique extension $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)$ of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to $F_3(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

PROOF: By Lemma B.29, Lemma B.32 and Lemma B.33.

⟨3⟩2. $F(C_E(D_{N_1} \otimes D_{N_2}(\alpha))) = F_3(C_E(D_{N_1} \otimes D_{N_2}(\alpha)))$

PROOF: By Proposition B.1.

⟨3⟩3. Q.E.D.

PROOF: By ⟨3⟩1, ⟨3⟩2 and the rule of replacement [51].

⟨2⟩2. $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)$ is finite.

⟨3⟩1. $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

⟨4⟩1. $D_{N_1} \otimes D_{N_2}(\alpha) \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

⟨5⟩1. $D_{N_1} \otimes D_{N_2}(\alpha) = c(\langle\rangle, D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By Definition 3.1.

⟨5⟩2. Q.E.D.

PROOF: By ⟨5⟩1 and Definition 3.3.

⟨4⟩2. $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By ⟨4⟩1, Lemma B.29, Lemma B.32 and Lemma B.33.

⟨4⟩3. $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1.$

PROOF: By definition (25) and Lemma 5.6.3.

⟨4⟩4. Q.E.D.

PROOF: By ⟨4⟩2, ⟨4⟩3 and the rule of replacement [51].

⟨3⟩2. Q.E.D.

PROOF: By ⟨3⟩1 and Definition A.6.

⟨2⟩3. $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha) = \sigma(F(C_E(D_{N_1} \otimes D_{N_2}(\alpha))))$

PROOF: By definition (23) and Lemma B.2.

⟨2⟩4. Q.E.D.

PROOF: By ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 and Theorem B.3, define $f_{N_1} \otimes f_{N_2}(\alpha)$ to be the unique extension of $\mu_{N_1} \otimes \mu_{N_2}'''(\alpha)$.

$\langle 1\rangle 2.$ Q.E.D.

Lemma B.34. *Let D be a non-empty set and $\mathcal{F}$ be a σ-field over D and let f be a measure on f. If $f(D) \leq 1$, then f is a conditional probability measure on $\mathcal{F}$.*

Proof:

$\langle 1\rangle 1.$ Assume: $f(D) \leq 1$

Prove: $\forall A \in \mathcal{F} : f(A) = 0 \lor \exists c \in \langle 0, 1]$ such that the function f' defined by $f'(A) = f(A)/c$ is a probability measure on $\mathcal{F}$.

$\langle 2\rangle 1.$ Case: $f(D) = 0$

$\langle 3\rangle 1.$ $\forall A \in \mathcal{F} : f(A) = 0$

$\langle 4\rangle 1.$ $\forall A \in \mathcal{F} : A \subseteq D$

Proof: By the fact that $\mathcal{F}$ is a σ-field over D, Definition A.4 and Definition A.3.

$\langle 4\rangle 2.$ Q.E.D.

Proof: By assumption $\langle 2\rangle 1$, $\langle 4\rangle 1$ and Lemma B.8.

$\langle 3\rangle 2.$ Q.E.D.

Proof: By $\langle 3\rangle 1$ and $\lor$ introduction.

$\langle 2\rangle 2.$ Case: $f(D) > 0$

$\langle 3\rangle 1.$ $\exists c \in \langle 0, 1]$ such that the function f' defined by $f'(A) = f(A)/c$ is a probability measure on $\mathcal{F}$

$\langle 4\rangle 1.$ $\exists n \in \langle 0, 1] : f(D) = n$

Proof: By assumption $\langle 1\rangle 1$, assumption $\langle 2\rangle 2$ and $\exists$ introduction.

$\langle 4\rangle 2.$ Let: $c \in \langle 0, 1]$ such that $f(D) = c$

Proof: By $\langle 4\rangle 1$.

$\langle 4\rangle 3.$ Let: $f'(A) = f(A)/c$

$\langle 4\rangle 4.$ f' is a probability measure on $\mathcal{F}$.

$\langle 5\rangle 1.$ $f'(\emptyset) = 0$

$\langle 6\rangle 1.$ $f(\emptyset) = 0$

Proof: By the fact that f is a measure, and Definition A.6.

$\langle 6\rangle 2.$ Q.E.D.

Proof: By $\langle 4\rangle 3$, $\langle 4\rangle 2$, $\langle 6\rangle 1$ and elementary arithmetic.

$\langle 5\rangle 2.$ $\forall \phi \in \mathbb{P}(\mathcal{H})^{\omega} : (\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}$
$\land (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\land \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F})$
$\Rightarrow f'(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f'(\phi[j])$

$\langle 6\rangle 1.$ Assume: $\phi \in \mathbb{P}(\mathcal{H})^{\omega}$

Prove: $(\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}$
$\land (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\land \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F})$
$\Rightarrow f'(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f'(\phi[j])$

$\langle 7\rangle 1.$ Assume: $\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}$
$\land (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$
$\land \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}$

Prove: $f'(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f'(\phi[j])$

$\langle 8\rangle 1.$ $f(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f(\phi[i])$

Proof: By assumption $\langle 7\rangle 1$, the fact that f is a measure and Definition A.6.

⟨8⟩2. $f(\bigcup_{j=1}^{\#\phi} \phi[j])/c = (\sum_{j=1}^{\#\phi} f(\phi[i]))/c$

PROOF:By ⟨8⟩1, ⟨4⟩2 and elementary arithmetic.

⟨8⟩3. $(\sum_{j=1}^{\#\phi} f(\phi[i]))/c = \sum_{j=1}^{\#\phi}(f(\phi[i])/c)$

⟨9⟩1. $\sum_{j=1}^{\#\phi} f(\phi[i]) \leq 1$

⟨10⟩1. $f(\bigcup_{j=1}^{\#\phi} \phi[j]) \leq 1$

⟨11⟩1. $\bigcup_{j=1}^{\#\phi} \phi[j] \subseteq D$

PROOF: By assumption ⟨7⟩1, the fact that $\mathcal{F}$ is a σ-field over D Definition A.4 and Definition A.3.

⟨11⟩2. Q.E.D.

PROOF: By assumption ⟨1⟩1, ⟨11⟩1 and Lemma B.8.

⟨10⟩2. Q.E.D.

PROOF: By ⟨8⟩1, ⟨10⟩1 and the rule of replacement [51].

⟨9⟩2. Q.E.D.

PROOF: By ⟨9⟩1 and elementary arithmetic.

⟨8⟩4. $\sum_{j=1}^{\#\phi}(f(\phi[i])/c) = \sum_{j=1}^{\#\phi} f'(\phi[j])$

⟨9⟩1. $\forall i \in [1..\#\phi] : f'(\phi[i]) = f(\phi[i])/c$

PROOF: By ⟨4⟩3.

⟨9⟩2. Q.E.D.

PROOF: By ⟨9⟩1 and the rule of equality between functions [51].

⟨8⟩5. Q.E.D.

PROOF: By ⟨4⟩3, ⟨8⟩2, ⟨8⟩3, ⟨8⟩4 and the rule of transitivity [51].

⟨7⟩2. Q.E.D.

PROOF: ⇒ introduction.

⟨6⟩2. Q.E.D.

PROOF: ∀ introduction.

⟨5⟩3. $f'(D) = 1$

PROOF: By ⟨4⟩2, ⟨4⟩3 and elementary arithmetic.

⟨5⟩4. Q.E.D.

PROOF: By ⟨5⟩1, ⟨5⟩2, ⟨5⟩3 and Definition A.7.

⟨4⟩5. Q.E.D.

PROOF: By ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 and ∃ introduction.

⟨3⟩2. Q.E.D.

PROOF: By ⟨3⟩1 and ∨ introduction.

⟨2⟩3. Q.E.D.

PROOF: By assumption ⟨1⟩1, the cases ⟨2⟩2 and ⟨2⟩1 are exhaustive.

⟨1⟩2. Q.E.D.

PROOF: ⇒ introduction.

Corollary 5.8 *Let $f_{N_1} \otimes f_{N_2}(\alpha)$ be the unique extension of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to the cone-σ-field $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$. Then $f_{N_1} \otimes f_{N_2}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.*

PROOF:

⟨1⟩1. $\forall A \in \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha) : f_{N_1} \otimes f_{N_2}(\alpha)(A) = 0 \vee \exists c \in \langle 0, 1]$ such that the function f' defined by $f'(A) = f_{N_1} \otimes f_{N_2}(\alpha)(A)/c$ is a probability measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.

⟨2⟩1. $f_{N_1} \otimes f_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$

⟨3⟩1. $D_{N_1} \otimes D_{N_2}(\alpha) \in C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

$\langle 4\rangle 1.$ $D_{N_1} \otimes D_{N_2}(\alpha) = c(\langle\rangle, D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By Definition 3.1.

$\langle 4\rangle 2.$ Q.E.D.

PROOF: By $\langle 4\rangle 1$ and Definition 3.3.

$\langle 3\rangle 2.$ $f_{N_1} \otimes f_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) = \mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By $\langle 3\rangle 1$, the fact that $f_{N_1} \otimes f_{N_2}(\alpha)$ is the unique extension of $\mu_{N_1} \otimes \mu_{N_2}(\alpha)$ to the cone-σ-field $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$ and Theorem B.3.

$\langle 3\rangle 3.$ $\mu_{N_1} \otimes \mu_{N_2}(\alpha)(D_{N_1} \otimes D_{N_2}(\alpha)) \leq 1$.

PROOF: By definition (25) and Lemma 5.6.3.

$\langle 3\rangle 4.$ Q.E.D.

PROOF: By $\langle 3\rangle 2$, $\langle 3\rangle 3$ and the rule of transitivity [51].

$\langle 2\rangle 2.$ Q.E.D.

PROOF: By $\langle 2\rangle 1$, the fact that $f_{N_1} \otimes f_{N_2}(\alpha)$ is a measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$ by Theorem 5.7 and Lemma B.34.

$\langle 1\rangle 2.$ Q.E.D.

Theorem 5.9 *Let N_1 and N_2 be two component such that $N_1 \cap N_2 = \emptyset$. Then $I_{N_1} \otimes I_{N_2}$ is a probabilistic component execution of $N_1 \cup N_2$.*

PROOF:

$\langle 1\rangle 1.$ $I_{N_1} \otimes I_{N_2}$ is a probabilistic component execution of $N_1 \cup N_2$

$\langle 2\rangle 1.$ $\forall \alpha \in \mathcal{B}_{N_1 \cup N_2} : I_{N_1} \otimes I_{N_2} = (D_{N_1} \otimes D_{N_2}(\alpha), \mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha), f_{N_1} \otimes f_{N_2}(\alpha))$

PROOF: By definition (26).

$\langle 2\rangle 2.$ LET: $\alpha \in \mathcal{B}_{N_1 \cup N_2}$

$\langle 2\rangle 3.$ $D_{N_1} \otimes D_{N_2}(\alpha)$ is the trace set of $I_{N_1} \otimes I_{N_2}(\alpha)$.

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\forall$ elimination and definition (22).

$\langle 2\rangle 4.$ $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$ is the cone-σ-field generated by $C_E(D_{N_1} \otimes D_{N_2}(\alpha))$

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\forall$ elimination and definition (23).

$\langle 2\rangle 5.$ $f_{N_1} \otimes f_{N_2}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{N_1} \otimes \mathcal{F}_{N_2}(\alpha)$.

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\forall$ elimination and Corollary 5.8.

$\langle 2\rangle 6.$ Q.E.D.

PROOF: By steps $\langle 2\rangle 1$ to $\langle 2\rangle 5$.

$\langle 1\rangle 2.$ Q.E.D.

B.4. Hiding

In the following we prove that components are closed under hiding of assets and interface names. That is, we show that hiding assets and/or interface names in a component yields a new component.

Lemma B.35. *The function $f_{\delta n\,:\,N}$ is defined for all elements in $C_E(D_{\delta n\,:\,N}(\alpha)) \backslash C(D_{\delta n\,:\,N}(\alpha))$. That is:*

$$\forall t_1 \in (\mathcal{H} \cap \mathcal{E}^*) : \{t_1\} \in C_E(D_{\delta n\,:\,N}(\alpha)) \setminus C(D_{\delta n\,:\,N}(\alpha)) \Rightarrow \\ \left\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \{t_1\}\right\} \in \mathcal{F}_N(\delta n : \alpha)$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $t_1 \in (\mathcal{H} \cap \mathcal{E}^*)$

PROVE: $\{t_1\} \in C_E(D_{\delta n\,:\,N}(\alpha)) \setminus C(D_{\delta n\,:\,N}(\alpha)) \Rightarrow$
$\left\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \{t_1\}\right\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 2\rangle 1.$ Assume: $\{t_1\} \in C_E(D_{\delta n\,:\,N}(\alpha)) \setminus C(D_{\delta n\,:\,N}(\alpha))$
Prove: $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 3\rangle 1.$ Let: $S = \big\{t' \in \mathcal{H} \cap \mathcal{E}^* \,|\, \exists t'' \in D_N(\delta n : \alpha) : t' \sqsubseteq t'' \wedge \mathcal{E}_{\delta n\,:\,N} \circledS\, t' = t_1\big\}$

$\langle 3\rangle 2.$ Let: $S'' = \big\{t' \in \mathcal{H} \cap \mathcal{E}^* \,|\, \exists t'' \in D_N(\delta n : \alpha) : t' \sqsubseteq t'' \wedge t_1 \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS\, t' \wedge \#\mathcal{E}_{\delta n\,:\,N} \circledS\, t' = \#t_1 + 1\big\}$

$\langle 3\rangle 3.$ $\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \setminus \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha)) \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 4\rangle 1.$ $\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \in \mathcal{F}_N(\delta n : \alpha)$
Proof: By $\langle 3\rangle 1$ and Corollary B.10.

$\langle 4\rangle 2.$ $\bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha)) \in \mathcal{F}_N(\delta n : \alpha)$
Proof: By $\langle 3\rangle 2$ and Corollary B.10.

$\langle 4\rangle 3.$ Q.E.D.
Proof: By $\langle 4\rangle 1$ and $\langle 4\rangle 2$, since $\mathcal{F}_N(\delta n : \alpha)$ is closed under set-difference.

$\langle 3\rangle 4.$ $\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \setminus \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha)) = \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\}$

$\langle 4\rangle 1.$ $\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \setminus \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha)) \subseteq \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\}$

$\langle 5\rangle 1.$ Assume: $t_2 \in \bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \setminus \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha))$
Prove: $t_2 \in \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\}$

$\langle 6\rangle 1.$ Assume: $t_2 \notin \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\}$
Prove: $\perp$

$\langle 7\rangle 1.$ $t_2 \in D_N(\delta n : \alpha)$
Proof: By assumption $\langle 5\rangle 1$, $\langle 3\rangle 1$ and Definition 3.1.

$\langle 7\rangle 2.$ $t_1 \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS\, t_2$
Proof: By assumption $\langle 1\rangle 1$, $\langle 3\rangle 1$ and assumption $\langle 5\rangle 1$.

$\langle 7\rangle 3.$ $t_1 \neq \mathcal{E}_{\delta n\,:\,N} \circledS\, t_2$
Proof: By assumption $\langle 6\rangle 1$ and $\langle 7\rangle 1$.

$\langle 7\rangle 4.$ $\#\mathcal{E}_{\delta n\,:\,N} \circledS\, t_2 > \#t_1$
Proof: By $\langle 7\rangle 2$ and $\langle 7\rangle 3$.

$\langle 7\rangle 5.$ $\exists t \in S'' : t \sqsubseteq t_2$
Proof: By $\langle 7\rangle 4$ and $\langle 7\rangle 2$ and $\langle 3\rangle 2$.

$\langle 7\rangle 6.$ $t_2 \in \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha))$
Proof: By $\langle 7\rangle 5$ and Definition 3.1.

$\langle 7\rangle 7.$ Q.E.D.
Proof: By assumption $\langle 5\rangle 1$, $\langle 7\rangle 6$ and $\perp$-introduction.

$\langle 6\rangle 2.$ Q.E.D.
Proof: Proof by contradiction.

$\langle 5\rangle 2.$ Q.E.D.
Proof: $\subseteq$-rule.

$\langle 4\rangle 2.$ $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\} \subseteq \bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \setminus \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha))$

$\langle 5\rangle 1.$ Assume: $t_2 \in \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in \{t_1\}\big\}$
Prove: $t_2 \in \bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \setminus \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha))$

$\langle 6\rangle 1.$ $t_2 \in \bigcup_{t' \in S} c(t', D_N(\delta n : \alpha))$

$\langle 7\rangle 1.$ $t_2 \in D_N(\delta n : \alpha)$
Proof: By assumption $\langle 5\rangle 1$.

$\langle 7\rangle 2.$ $\mathcal{E}_{\delta n\,:\,N} \circledS\, t_2 = t_1$

PROOF: By assumption $\langle 5\rangle 1$

$\langle 7\rangle 3.$ Q.E.D.

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 3\rangle 1$.

$\langle 6\rangle 2.$ $t_2 \notin \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha))$

$\langle 7\rangle 1.$ ASSUME: $t_2 \in \bigcup_{t'' \in S''} c(t'', D_N(\delta n : \alpha))$

PROVE: $\perp$

$\langle 8\rangle 1.$ $\mathcal{E}_{\delta n\,:\,N} \circledS\, t_2 = t_1$

PROOF: By assumption $\langle 5\rangle 1$

$\langle 8\rangle 2.$ $\exists t' \in D_{\delta n\,:\,N}(\alpha) : t' \sqsubseteq t_2 \wedge t_1 \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS\, t' \wedge$
$\#\mathcal{E}_{\delta n\,:\,N} \circledS\, t' = \#t_1 + 1$

PROOF: By assumption $\langle 7\rangle 1$ and $\langle 3\rangle 2$.

$\langle 8\rangle 3.$ $\mathcal{E}_{\delta n\,:\,N} \circledS\, t_2 \neq t_1$

$\langle 9\rangle 1.$ $\#\mathcal{E}_{\delta n\,:\,N} \circledS\, t_2 > \#t_1$

PROOF: By $\langle 8\rangle 2$.

$\langle 9\rangle 2.$ Q.E.D.

PROOF: By $\langle 9\rangle 1$.

$\langle 8\rangle 4.$ Q.E.D.

PROOF: By $\langle 8\rangle 1$, $\langle 8\rangle 3$ and $\perp$-introduction.

$\langle 7\rangle 2.$ Q.E.D.

PROOF: Proof by contradiction.

$\langle 6\rangle 3.$ Q.E.D.

PROOF: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$.

$\langle 5\rangle 2.$ Q.E.D.

PROOF: $\subseteq$-rule.

$\langle 4\rangle 3.$ Q.E.D.

PROOF: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and the $=$-rule for sets [29].

$\langle 3\rangle 5.$ Q.E.D.

PROOF: By $\langle 3\rangle 3$, $\langle 3\rangle 4$ and the rule of replacement [51].

$\langle 2\rangle 2.$ Q.E.D.

PROOF: $\Rightarrow$-introduction.

$\langle 1\rangle 2.$ Q.E.D.

PROOF: $\forall$-introduction.

Lemma B.36. *The function $f_{\delta n\,:\,N}$ is defined for all elements in $C(D_{\delta n\,:\,N}(\alpha))$. That is:*

$$\forall t_1 \in (\mathcal{H} \cap \mathcal{E}^*) : c(t_1, D_{\delta n\,:\,N}(\alpha)) \in C(D_{\delta n\,:\,N}(\alpha)) \Rightarrow \\ \left\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\right\} \in \mathcal{F}_N(\delta n : \alpha)$$

PROOF:

$\langle 1\rangle 1.$ ASSUME: $t_1 \in (\mathcal{H} \cap \mathcal{E}^*)$

PROVE: $c(t_1, D_{\delta n\,:\,N}(\alpha)) \in C(D_{\delta n\,:\,N}(\alpha))$
$\Rightarrow \left\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\right\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 2\rangle 1.$ ASSUME: $c(t_1, D_{\delta n\,:\,N}(\alpha)) \in C(D_{\delta n\,:\,N}(\alpha))$

PROVE: $\left\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS\, t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\right\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 3\rangle 1.$ LET: $S = \left\{t' \in \mathcal{H} \cap \mathcal{E}^* \,|\, \exists t'' \in D_N(\delta n : \alpha) : t_1 \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS\, t'' \wedge t' \sqsubseteq t'' \wedge\right.$
$\left.\mathcal{E}_{\delta n\,:\,N} \circledS\, t' = t_1\right\}$

⟨3⟩2. $\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \in \mathcal{F}_N(\delta n : \alpha)$

Proof: By ⟨3⟩1 and Corollary B.10.

⟨3⟩3. $\bigcup_{t' \in S} c(t', D_N(\epsilon n : \alpha)) = \{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\}$

⟨4⟩1. $\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha)) \subseteq \{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\}$

⟨5⟩1. Assume: $t_2 \in \bigcup_{t' \in S} c(t', D_N(\delta n : \alpha))$

Prove: $t_2 \in \{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\}$

⟨6⟩1. $t_2 \in D_N(\delta n : \alpha)$

Proof: By assumption ⟨5⟩1 and Definition 3.1.

⟨6⟩2. $\mathcal{E}_{\delta n\,:\,N} \circledS t_2 \in c(t_1, D_{\delta n\,:\,N}(\alpha))$

⟨7⟩1. $\mathcal{E}_{\delta n\,:\,N} \circledS t_2 \in D_{\delta n\,:\,N}(\alpha)$

Proof: By ⟨6⟩1 and Definition 7.1.

⟨7⟩2. $t_1 \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS t_2$

⟨8⟩1. $\exists t' \in \mathcal{H} : t' \sqsubseteq t_2 \wedge \mathcal{E}_{\delta n\,:\,N} \circledS t' = t_1$

Proof: By assumption ⟨5⟩1 and ⟨3⟩1.

⟨8⟩2. Let: t' be a trace such that $t' \sqsubseteq t_2 \wedge \mathcal{E}_{\delta n\,:\,N} \circledS t' = t_1$

Proof: By ⟨8⟩1.

⟨8⟩3. $\mathcal{E}_{\delta n\,:\,N} \circledS t' \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS t_2$

Proof: By ⟨8⟩2 and definition (7).

⟨8⟩4. Q.E.D.

Proof: By ⟨8⟩2, ⟨8⟩3 and the rule of replacement [51].

⟨7⟩3. Q.E.D.

Proof: By ⟨7⟩2, ⟨7⟩1 and Definition 3.1.

⟨6⟩3. Q.E.D.

Proof: By ⟨6⟩1 and ⟨6⟩2.

⟨5⟩2. Q.E.D.

Proof: $\subseteq$-rule [29].

⟨4⟩2. $\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\} \subseteq$
$\bigcup_{t' \in S} c(t', D_N(\delta n : \alpha))$

⟨5⟩1. Assume: $t_2 \in \{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c(t_1, D_{\delta n\,:\,N}(\alpha))\}$

Prove: $t_2 \in \bigcup_{t' \in S} c(t', D_N(\epsilon n : \alpha))$

⟨6⟩1. $\exists t \in S : t \sqsubseteq t_2$

⟨7⟩1. $t_2 \in D_N(\delta n : \alpha)$

Proof: By ⟨5⟩1.

⟨7⟩2. $t_1 \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS t_2$

⟨8⟩1. $\mathcal{E}_{\delta n\,:\,N} \circledS t_2 \in c(t_1, D_{\delta n\,:\,N}(\alpha))$

Proof: By ⟨5⟩1.

⟨8⟩2. Q.E.D.

Proof: By ⟨8⟩1 and Definition 3.1.

⟨7⟩3. $\exists t'' \in \mathcal{H} \cap \mathcal{E}^* : t'' \sqsubseteq t_2 \wedge \mathcal{E}_{\delta n\,:\,N} \circledS t'' = t_1$

⟨8⟩1. $t_1 = \mathcal{E}_{\delta n\,:\,N} \circledS t_2|_{\#t_1}$

Proof: By ⟨7⟩2 and definition (2).

⟨8⟩2. $\mathcal{E}_{\delta n\,:\,N} \circledS t_2|_{\#t_1} \sqsubseteq \mathcal{E}_{\delta n\,:\,N} \circledS t_2$

Proof: By ⟨7⟩2, ⟨8⟩1 and the rule of replacement [51].

⟨8⟩3. $\#\mathcal{E}_{\delta n\,:\,N} \circledS t_2|_{\#t_1} \in \mathbb{N}$

Proof: By assumption ⟨1⟩1, ⟨8⟩1 and the rule of replacement [51].

⟨8⟩4. Q.E.D.

Proof: By $\langle 8\rangle 2$, $\langle 8\rangle 1$, $\langle 8\rangle 3$ and $\exists$-introduction.

$\langle 7\rangle 4.$ Let: $t'' \in \mathcal{H} \cap \mathcal{E}^*$ such that $t'' \sqsubseteq t_2 \wedge \mathcal{E}_{\delta n\,:\,N} \circledS t'' = t_1$
Proof: By $\langle 7\rangle 3$.

$\langle 7\rangle 5.$ $t'' \in S$
Proof: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 7\rangle 4$.

$\langle 7\rangle 6.$ Q.E.D.
Proof: By $\langle 7\rangle 4$, $\langle 7\rangle 5$ and $\exists$ introduction

$\langle 6\rangle 2.$ Q.E.D.
Proof: By $\langle 6\rangle 1$ and Definition 3.1.

$\langle 5\rangle 2.$ Q.E.D.
Proof: $\subseteq$-rule [29].

$\langle 4\rangle 3.$ Q.E.D.
Proof: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and the $=$-rule for sets [29].

$\langle 3\rangle 4.$ Q.E.D.
Proof: By $\langle 3\rangle 2$, $\langle 3\rangle 3$ and the rule of replacement [51].

$\langle 2\rangle 2.$ Q.E.D.
Proof: $\Rightarrow$-introduction.

$\langle 1\rangle 2.$ Q.E.D.
Proof: $\forall$-introduction.

Corollary B.37. *The function $f_{\delta n\,:\,N}$ is defined for all elements in $C_E(D_{\delta n\,:\,N}(\alpha))$. That is:*

$$\forall c \in \mathbb{P}(\mathcal{H}) : c \in C_E(D_{\delta n\,:\,N}(\alpha)) \Rightarrow \\ \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\big\} \in \mathcal{F}_N(\delta n : \alpha)$$

Proof. By Lemma B.35 and B.36.

Lemma B.38. *The function $f_{\delta n\,:\,N}$ is well defined. That is:*

$$\forall c \in \mathbb{P}(\mathcal{H}_{\delta n\,:\,N}) : c \in \mathcal{F}_{\delta n\,:\,N}(\alpha) \Rightarrow \\ \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\big\} \in \mathcal{F}_N(\delta n : \alpha)$$

Proof:

$\langle 1\rangle 1.$ Assume: $c \in \mathbb{P}(\mathcal{H}_{\delta n\,:\,N})$
Prove: $c \in \mathcal{F}_{\delta n\,:\,N}(\alpha) \Rightarrow \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\big\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 2\rangle 1.$ Assume: $c \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$
Prove: $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\big\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 3\rangle 1.$ c is a countable union of elements in $C_E(D_{\delta n\,:\,N}(\alpha))$.
Proof: By $\langle 2\rangle 1$ and Lemma B.14.

$\langle 3\rangle 2.$ Let: ϕ be a sequence of cones in $C_E(D_{\delta n\,:\,N}(\alpha))$ such that $c = \bigcup_{i=1}^{\#\phi} \phi[i]$.
Proof: By $\langle 3\rangle 1$ and Definition A.1.

$\langle 3\rangle 3.$ $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{i=1}^{\#\phi} \phi[i]\big\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 4\rangle 1.$ $\forall i \in [1..\#\phi] : \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\} \in \mathcal{F}_N(\delta n : \alpha)$
Proof: By Lemma B.37.

$\langle 4\rangle 2.$ $\bigcup_{i=1}^{\#\phi} \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\} \in \mathcal{F}_N(\delta n : \alpha)$

PROOF: By ⟨3⟩2 and ⟨4⟩1, since $\mathcal{F}_N(\delta n : \alpha)$ is closed under countable union.

⟨4⟩3. $\bigcup_{i=1}^{\#\phi}\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\} =$
$\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{i=1}^{\#\phi} \phi[i]\}$

PROOF: By definition (7).

⟨4⟩4. Q.E.D.

PROOF: By ⟨4⟩2, ⟨4⟩3 and the rule of replacement [51].

⟨3⟩4. Q.E.D.

PROOF: By ⟨3⟩2, ⟨3⟩3 and the rule of replacement [51].

⟨2⟩2. Q.E.D.

PROOF: ⇒-introduction.

⟨1⟩2. Q.E.D.

PROOF: ∀-introduction.

Lemma B.39. *Let N be a component and let α be a queue history in $\mathcal{B}_N$. Then*

1. *$D_{\exists n\,:\,N}(\alpha)$ is a set of well-formed traces*
2. *$\mathcal{F}_{\exists n:N}(\alpha)$ is the cone-σ-field of $D_{\exists n\,:\,N}(\alpha)$*
3. *$f_{\exists n\,:\,N}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{\exists n\,:\,N}(\alpha)$*

PROOF: (Proof of Lemma B.39.1.)

⟨1⟩1. $D_{\delta n\,:\,N}(\alpha)$ is a set of well-formed traces, that is, sequences of events fulfilling well-formedness constraints (8), (9) and (10).

⟨2⟩1. $D_{\delta n\,:\,N}(\alpha) = \{\mathcal{E}_{\delta n\,:\,N} \circledS t | t \in D_N(\delta n : \alpha)\}$

PROOF: By Definition 7.1.

⟨2⟩2. $\{\mathcal{E}_{\delta n\,:\,N} \circledS t | t \in D_N(\delta n : \alpha)\}$ is a set of well-formed traces.

⟨3⟩1. $D_N(\delta n : \alpha)$ is a set of well-formed traces.

PROOF: By definition (26).

⟨3⟩2. $\forall t \in \{\mathcal{E}_{\delta n\,:\,N} \circledS t | t \in D_N(\delta n : \alpha)\} : (\forall i, j \in \{1..\#t\} : i < j \Rightarrow q.t[i] < q.t[j]) \wedge (\#t = \infty \Rightarrow \forall k \in \mathcal{Q} : \exists i \in \mathbb{N} : q.t[i] > k)$

PROOF: By ⟨3⟩1 and definition (7), since the filtering of a trace with regard to a set of events does not change the ordering of the remaining events in the trace.

⟨3⟩3. $\forall t \in \{\mathcal{E}_{\delta n\,:\,N} \circledS t | t \in D_N(\delta n : \alpha)\} : \forall l, m \in \mathsf{in}(N) \setminus \{n\} :$

LET: $i = (\{?\} \times (\mathcal{S} \times l \times m \times \mathcal{Q})) \circledS t$
$o = (\{!\} \times (\mathcal{S} \times l \times m \times \mathcal{Q})) \circledS t$

⟨3⟩4. $\forall j \in \{1..\#i\} : q.o[j] < q.i[j]$

PROOF: By ⟨3⟩1, ⟨3⟩3 and definition (7), since the filtering of a trace with regard to a set of events does not change the ordering of the remaining events in the trace.

⟨3⟩5. $\Pi_{\{1,2,3\}}.(\Pi_{\{2\}}.i) \sqsubseteq \Pi_{\{1,2,3\}}.(\Pi_{\{2\}}.o)$, that is, the sequence of consumed messages sent from an internal interface l to another internal interface m, is a prefix of the sequence of transmitted messages from l to m, when disregarding time.

PROOF: By ⟨3⟩1 this constraint is fulfilled by all traces in $D_N(\delta n : \alpha)$. The new traces are obtained by filtering away messages consumed by or transmitted from n. Hence, n is treated as an external interface. The remaining internal communication is not affected by the filtering of events, so the restriction is fulfilled by the new traces.

⟨3⟩6. Q.E.D.

PROOF: By ⟨3⟩2, ⟨3⟩4 and ⟨3⟩5.

⟨2⟩3. Q.E.D.

PROOF: By ⟨2⟩1, ⟨2⟩2 and the rule of replacement [51].

⟨1⟩2. Q.E.D.

PROOF: (Proof of Lemma B.39.2.)

⟨1⟩1. $\mathcal{F}_{\delta n:N}(\alpha) = \sigma(C_E(D_{\delta n\,:\,N}(\alpha)))$ that is, the cone-σ-field of $D_{\delta n\,:\,N}(\alpha)$.

PROOF: By Definition 7.1.

⟨1⟩2. Q.E.D.

PROOF: (Proof of Lemma B.39.3.)

⟨1⟩1. $f_{\delta n\,:\,N}(\alpha)$ is a conditional probability measure on $\mathcal{F}_{\delta n\,:\,N}(\alpha)$.

⟨2⟩1. $f_{\delta n\,:\,N}(\alpha)$ is a measure on $\mathcal{F}_{\delta n\,:\,N}(\alpha)$.

⟨3⟩1. $f_{\delta n\,:\,N}(\alpha)$ is well defined, that is

$\forall c \in \mathbb{P}(\mathbb{P}(\mathcal{H}_{\delta n\,:\,N})) : c \in \mathcal{F}_{\delta n\,:\,N}(\alpha) \Rightarrow$

$\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in c\big\} \in \mathcal{F}_N(\delta n : \alpha)$

PROOF: By Lemma B.38.

⟨3⟩2. $f_{\delta n\,:\,N}(\alpha)(\emptyset) = 0$

⟨4⟩1. $f_{\delta n\,:\,N}(\alpha)(\emptyset) = f_N(\delta n : \alpha)(\emptyset)$

PROOF: By Definition 7.1.

⟨4⟩2. $f_N(\delta n : \alpha)(\emptyset) = 0$

PROOF: By the fact that N is a component, Definition 6.1 and Definition 5.3.

⟨4⟩3. Q.E.D.

PROOF: By ⟨4⟩1, ⟨4⟩2 and the rule of transitivity [51].

⟨3⟩3. $\forall \phi \in \mathbb{P}(\mathcal{H})^{\omega} : (\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$

$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$

$\wedge\, \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha))$

$\Rightarrow f_{\delta n\,:\,N}(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f_{\delta n\,:\,N}(\alpha)(\phi[j])$

⟨4⟩1. ASSUME: $\phi \in \mathbb{P}(\mathcal{H})^{\omega}$

PROVE: $(\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$

$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$

$\wedge\, \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha))$

$\Rightarrow f_{\delta n\,:\,N}(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f_{\delta n\,:\,N}(\alpha)(\phi[j])$

⟨5⟩1. ASSUME: $\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$

$\wedge\, (\forall m, j \in [1..\#\phi] : j \neq m \Rightarrow \phi[j] \cap \phi[m] = \emptyset)$

$\wedge\, \bigcup_{i=1}^{\#\phi} \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$

PROVE: $f_{\delta n\,:\,N}(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) = \sum_{j=1}^{\#\phi} f_{\delta n\,:\,N}(\alpha)(\phi[j])$

⟨6⟩1. $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{j=1}^{\#\phi} \phi[j]\big\} \in \mathcal{F}_N(\delta n : \alpha)$

PROOF: By assumption ⟨5⟩1 ($\bigcup_{j=1}^{\#\phi} \phi[j] \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$) and Lemma B.38.

⟨6⟩2. $\forall i \in [1..\#\phi] : \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\} \in \mathcal{F}_N(\delta n : \alpha)$

PROOF: By assumption ⟨5⟩1 ($\forall i \in [1..\#\phi] : \phi[i] \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$) and Lemma B.38.

⟨6⟩3. $f_{\delta n\,:\,N}(\alpha)(\bigcup_{j=1}^{\#\phi} \phi[j]) =$

$f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{j=1}^{\#\phi} \phi[j]\big\})$

PROOF: By Definition 7.1 and ⟨6⟩1.

⟨6⟩4. $f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{j=1}^{\#\phi} \phi[j]\big\}) =$

$\sum_{j=1}^{\#\phi} f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\})$

⟨7⟩1. $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{j=1}^{\#\phi} \phi[j]\big\} =$
$\bigcup_{j=1}^{\#\phi} \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\}$

Proof: By definition (7).

⟨7⟩2. $f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \bigcup_{j=1}^{\#\phi} \phi[j]\big\}) =$
$f_N(\delta n : \alpha)(\bigcup_{j=1}^{\#\phi} \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\})$

Proof: By ⟨7⟩1 and the rule of equality between functions [51].

⟨7⟩3. $f_N(\delta n : \alpha)(\bigcup_{j=1}^{\#\phi} \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\}) =$
$\sum_{j=1}^{\#\phi} f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\})$

⟨8⟩1. $\bigcup_{j=1}^{\#\phi} \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\} \in \mathcal{F}_N(\delta n : \alpha)$

Proof: By ⟨7⟩1, ⟨6⟩1 and the rule of replacement [51].

⟨8⟩2. $\forall j, m \in [1..\#\phi] : j \neq m \Rightarrow \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[j]\big\} \cap \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[m]\big\} = \emptyset$

⟨9⟩1. Assume: $\exists j, m \in [1..\#\phi] :$
$\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[j]\big\} \cap$
$\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[m]\big\} \neq \emptyset$

Prove: $\perp$

⟨10⟩1. Let: $j, m \in [1..\#\phi]$ such that
$\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[j]\big\} \cap$
$\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[m]\big\} \neq \emptyset$

Proof: By assumption ⟨9⟩1.

⟨10⟩2. $\exists t_1 \in D_N(\delta n : \alpha) :$
$t_1 \in \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[j]\big\} \wedge$
$t_1 \in \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[m]\big\}$

Proof: By ⟨10⟩1 and elementary set theory.

⟨10⟩3. Let: $t_1 \in D_N(\delta n : \alpha)$ such that
$t_1 \in \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[j]\big\} \wedge$
$t_1 \in \big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[m]\big\}$

Proof: By ⟨10⟩2.

⟨10⟩4. $\mathcal{E}_{\delta n\,:\,N} \circledS t_1 \in \phi[j] \wedge \mathcal{E}_{\delta n\,:\,N} \circledS t_1 \in \phi[m]$

Proof: By ⟨10⟩3.

⟨10⟩5. $\phi[j] \cap \phi[m] \neq \emptyset$

Proof: By ⟨10⟩4.

⟨10⟩6. Q.E.D.

Proof: By assumption ⟨5⟩1, ⟨10⟩5 and $\perp$-introduction.

⟨9⟩2. Q.E.D.

Proof: Proof by contradiction.

⟨8⟩3. Q.E.D.

Proof: By ⟨8⟩1, ⟨6⟩2 and ⟨8⟩2, the fact that N is a component, Definition 6.1 and Definition 5.3.

⟨7⟩4. Q.E.D.

Proof: By ⟨7⟩2, ⟨7⟩3 and the rule of transitivity.

⟨6⟩5. $\sum_{j=1}^{\#\phi} f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\}) =$
$\sum_{j=1}^{\#\phi} f_{\delta n\,:\,N}(\alpha)(\phi[j])$

$\langle 7\rangle 1.$ $\forall i \in [1..\#\phi] : f_{\delta n\,:\,N}(\alpha)(\phi[i]) =$
$f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in \phi[i]\big\})$

Proof: By Definition 7.1 and $\langle 6\rangle 2$.

$\langle 7\rangle 2.$ Q.E.D.

Proof: By $\langle 7\rangle 1$ and the rule of equality between functions [51].

$\langle 6\rangle 6.$ Q.E.D.

Proof: By $\langle 6\rangle 3$, $\langle 6\rangle 4$, $\langle 6\rangle 5$ and the rule of transitivity [51].

$\langle 5\rangle 2.$ Q.E.D.

Proof: $\Rightarrow$ rule.

$\langle 4\rangle 2.$ Q.E.D.

Proof: $\forall$-introduction

$\langle 3\rangle 4.$ Q.E.D.

Proof: By $\langle 3\rangle 1$, $\langle 3\rangle 2$ and $\langle 3\rangle 3$ and Definition A.6.

$\langle 2\rangle 2.$ $f_{\delta n\,:\,N}(\alpha)(D_{\delta n\,:\,N}(\alpha)) \leq 1$

$\langle 3\rangle 1.$ $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in D_{\delta n\,:\,N}(\alpha)\big\} \in \mathcal{F}_N(\delta n : \alpha)$

$\langle 4\rangle 1.$ $D_{\delta n\,:\,N}(\alpha) \in \mathcal{F}_{\delta n\,:\,N}(\alpha)$

Proof: By Definition 7.1 ($\mathcal{F}_{\delta n\,:\,N}(\alpha)$ is the cone-σ-field of $D_{\delta n\,:\,N}(\alpha)$).

$\langle 4\rangle 2.$ Q.E.D.

Proof: By $\langle 4\rangle 1$ and Lemma B.38.

$\langle 3\rangle 2.$ $f_{\delta n\,:\,N}(\alpha)(D_{\delta n\,:\,N}(\alpha)) = f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in D_{\delta n\,:\,N}(\alpha)\big\})$

Proof: By Definition 7.1 and $\langle 3\rangle 1$.

$\langle 3\rangle 3.$ $f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in D_{\delta n\,:\,N}(\alpha)\big\}) \leq 1$

$\langle 4\rangle 1.$ $f_N(\delta n : \alpha)(D_N(\delta n : \alpha)) \leq 1$

Proof: By the fact that N is a component, Definition 6.1, Definition 5.3 and Definition 5.2.

$\langle 4\rangle 2.$ $f_N(\delta n : \alpha)(\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in D_{\delta n\,:\,N}(\alpha)\big\}) =$
$f_N(\delta n : \alpha)(D_N(\delta n : \alpha))$

$\langle 5\rangle 1.$ $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in D_{\delta n\,:\,N}(\alpha)\big\} = D_N(\delta n : \alpha)$

$\langle 6\rangle 1.$ $\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in D_{\delta n\,:\,N}(\alpha)\big\} =$
$\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in (\mathcal{E}_{\delta n\,:\,N} \circledS D_N(\delta n : \alpha))\}$

$\langle 7\rangle 1.$ $D_{\delta n\,:\,N}(\alpha) = \mathcal{E}_{\delta n\,:\,N} \circledS D_N(\delta n : \alpha)$

Proof: By Definition 7.1 and definition (7).

$\langle 7\rangle 2.$ Q.E.D.

Proof: By $\langle 7\rangle 1$ and the rule of replacement [51].

$\langle 6\rangle 2.$ $\big\{t \in D_N(\delta n : \alpha) | \mathcal{E}_{\delta n\,:\,N} \circledS t \in (\mathcal{E}_{\delta n\,:\,N} \circledS D_N(\delta n : \alpha))\big\} = D_N(\delta n : \alpha)$

Proof: By definition (7).

$\langle 6\rangle 3.$ Q.E.D.

Proof: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and the rule of transitivity [51].

$\langle 5\rangle 2.$ Q.E.D.

Proof: By $\langle 5\rangle 1$ and the rule of equality between functions [51].

$\langle 4\rangle 3.$ Q.E.D.

Proof: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and the rule of transitivity [51].

$\langle 3\rangle 4.$ Q.E.D.

Proof: By $\langle 3\rangle 2$, $\langle 3\rangle 3$ and the rule of transitivity [51].

$\langle 2\rangle 3.$ Q.E.D.

Proof: By $\langle 2\rangle 1$, $\langle 2\rangle 2$ and Lemma B.34

⟨1⟩2. Q.E.D.

Lemma 7.2 *If I_N is a probabilistic component execution and n is an interface name, then $\delta n : I_N$ is a probabilistic component execution.*

Proof. Follows from Lemma B.39.1 to Lemma B.39.3.

Theorem 7.4 *If N is a component and a is an asset, then $\sigma a : N$ is a component.*

Proof:

⟨1⟩1. Assume: (I_N, A_N, cv_N, rf_N) is a component and a is an asset.
Prove: $\sigma a :(I_N, A_N, cv_N, rf_N)$ is a component, that is, a quadruple consisting of its probabilistic component execution, its assets, consequence function and risk function according to Definition 6.1.

⟨2⟩1. $\sigma a :(I_N, A_N, cv_N, rf_N) = (I_N, \sigma a : A_N, \sigma a : cv_N, \sigma a : rf_N)$
Proof: By Definition 7.3.

⟨2⟩2. $(I_N, \sigma a : A_N, \sigma a : cv_N, \sigma a : rf_N)$ is a component.

⟨3⟩1. I_N is a component execution.
Proof: By assumption ⟨1⟩1.

⟨3⟩2. $\sigma a : A_N$ is a set of assets.

⟨4⟩1. $\sigma a : A_N = A_N \setminus \{a\}$
Proof: By Definition 7.3.

⟨4⟩2. A_N is a set of assets.
Proof: By assumption ⟨1⟩1.

⟨4⟩3. Q.E.D.
Proof: By ⟨4⟩1 and ⟨4⟩2.

⟨3⟩3. $\sigma a : cv_N$ is a consequence function in $\mathcal{E}_N \times \sigma a : A_N \rightarrow \mathbb{N}$

⟨4⟩1. $\sigma a : cv_N = cv_N \setminus \{(e, a) \rightarrow c | e \in \mathcal{E} \wedge c \in \mathbb{N}\}$
Proof: By Definition 7.3.

⟨4⟩2. cv_N is a consequence function in $\mathcal{E}_N \times A_N \rightarrow \mathbb{N}$.
Proof: By assumption ⟨1⟩1.

⟨4⟩3. Q.E.D.
Proof: By ⟨4⟩1 and ⟨4⟩2.

⟨3⟩4. $\exists a : rf_N$ is a risk function in $\mathbb{N} \times [0, 1] \times \sigma a : A_N \rightarrow \mathbb{N}$

⟨4⟩1. $\sigma a : rf_N = rf_N \setminus \{(c, p, a) \rightarrow r | c, r \in \mathbb{N} \wedge p \in [0, 1]\}$
Proof: By Definition 7.3.

⟨4⟩2. rf_N is a risk function in $\mathbb{N} \times [0, 1] \times A_N \rightarrow \mathbb{N}$.
Proof: By assumption ⟨1⟩1.

⟨4⟩3. Q.E.D.
Proof: By ⟨4⟩1 and ⟨4⟩2.

⟨3⟩5. Q.E.D.
Proof: By ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, and ⟨3⟩4.

⟨2⟩3. Q.E.D.
Proof: By ⟨2⟩1, ⟨2⟩2 and the rule of replacement [51].

⟨1⟩2. Q.E.D.
Proof: ⇒-introduction.

Theorem 7.6 *If N is a component and n is an interface name, then $\delta n : N$ is a component.*

PROOF:

$\langle 1\rangle 1.$ ASSUME: (I_N, A_N, cv_N, rf_N) is a component and n is an interface name.
PROVE: $\delta n :(I_N, A_N, cv_N, rf_N)$ is a component.

$\langle 2\rangle 1.$ $\delta n :(I_N, A_N, cv_N, rf_N) = (\delta n : I_N, \sigma A_n : A_N, \sigma A_n : cv_N, \sigma A_n : rf_N)$
PROOF: By Definition 7.5.

$\langle 2\rangle 2.$ $(\delta n : I_N, \sigma A_n : A_N, \sigma A_n : cv_N, \sigma A_n : rf_N)$ is a component

$\langle 3\rangle 1.$ $\delta n : I_N(\alpha)$ is a probabilistic component execution.
PROOF: By Lemma 7.2.

$\langle 3\rangle 2.$ $(I_N, \sigma A_n : A_N, \sigma A_n : cv_N, \sigma A_n : rf_N)$ is a component.

$\langle 4\rangle 1.$ $\sigma A_n :(I_N, A_N, cv_N, rf_N)$ is a component.
PROOF: By assumption $\langle 1\rangle 1$ and Theorem 7.4.

$\langle 4\rangle 2.$ $\sigma A_n :(I_N, A_N, cv_N, rf_N) = (I_N, \sigma A_n : A_N, \sigma A_n : cv_N, \sigma A_n : rf_N)$
PROOF: By Definition 7.3.

$\langle 4\rangle 3.$ Q.E.D.
PROOF: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and the rule of replacement.

$\langle 3\rangle 3.$ $\sigma A_n : A_N$ is a set of assets,
$\sigma A_n : cv_N$ is a consequence function in $\mathcal{E}_N \times \sigma A_n : A_N \rightarrow \mathbb{N}$ and
$\sigma A_n : rf_N$ is a risk function in $\mathbb{N} \times [0, 1] \times \sigma A_n : A_N \rightarrow \mathbb{N}$
PROOF: By $\langle 3\rangle 2$ and Definition 6.1.

$\langle 3\rangle 4.$ Q.E.D.
PROOF: By $\langle 3\rangle 1$, $\langle 3\rangle 3$ and Definition 6.1.

$\langle 2\rangle 3.$ Q.E.D.
PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$ and the rule of replacement [51].

$\langle 1\rangle 2.$ Q.E.D.
PROOF: $\Rightarrow$-introduction.