University of Oslo
Department of Informatics

# Relating computer systems to sequence diagrams with underspecification, inherent nondeterminism and probabilistic choice

## Part 2

Atle Refsdal,
Ragnhild Kobro Runde,
Ketil Stølen

Research Report 347

ISBN 82-7368-304-4
ISSN 0806-3036

December 21, 2007

# Relating computer systems to sequence diagrams with underspecification, inherent nondeterminism and probabilistic choice

## Part 2: probabilistic choice

Atle Refsdal[1,2], Ragnhild Kobro Runde[1], Ketil Stølen[1,2]

[1] Department of Informatics, University of Oslo, Norway
[2] SINTEF ICT, Norway

**Abstract.** Having a sequence diagram specification and a computer system, we need to answer the question: *Is the system compliant with the sequence diagram specification in the desired way?* We present a procedure for answering this question for three variations of sequence diagrams. The procedure does not require access to information about the internals of the system such as program code.
The semantics of sequence diagrams is denotational and based on traces. In order to answer the initial question, the procedure starts by obtaining a basic representation of the system by e.g. testing. This representation is then transformed into the same semantic model as that used for the sequence diagram. Finally, a formal definition of compliance is applied to determine whether the system complies with the specification.
Compliance is closely related to refinement, and the definitions of compliance are based on refinement definitions. Therefore refinement as well as compliance is addressed. Compliance is not identical to refinement due to the partial nature of sequence diagram specifications.
The work is split in two parts. Part 1 [RRS07] introduces the necessary definitions for using the compliance checking procedure on sequence diagrams with underspecification and sequence diagrams with inherent nondeterminism. This paper presents Part 2, in which we introduce the necessary definitions for using the compliance checking procedure on sequence diagrams with probabilistic choice. Part 1 is a necessary prerequisite for Part 2.

## 1 Introduction

Having a sequence diagram specification and a computer system, we need to answer the question: *Is the system compliant with the specification in the desired way?*

Sequence diagrams are widely used for specifying computer systems within a broad range of application domains. They are used for different methodological purposes including requirements capture, illustrating example runs, test scenario specification and risk scenario documentation. Although sequence diagrams are widely used in practice, their relationship to real computer systems is nevertheless surprisingly unclear. This is partly caused by the fact that sequence diagrams are used for different purposes, but even more so because in contrast to most other techniques for specifying dynamic behaviour they give only a partial view.

Answering the initial question above requires an understanding of what is meant by a computer system and to what extent such a system is different from a sequence diagram. Obviously, we need a formal model for computer systems. Also, the answer clearly depends on the expressiveness of the sequence diagram dialect we are using. In this paper we study the problem with respect to sequence diagrams with probabilistic choice, as formally defined in the denotational trace semantics of probabilistic STAIRS (pSTAIRS) [RHS07a].

The notion of compliance is closely related to that of refinement. Whereas compliance relates a specification to (a mathematical representation of) a system, refinement is a way of relating different specifications of the same system at different levels of abstraction. The idea is that a refinement should be a more detailed description containing all the constraints given by the original specification, in addition to some new ones.[3] Different development stages may require different notions of refinement. For example, in early stages one may wish to allow introduction of new alternative ways to solve a certain task (i.e. to introduce more underspecification). Toward the end of the development process the only allowed refinement might be to decide on how each task will actually be solved, which amounts to removing underspecification by making design decisions. The final specification used when implementing the system is the result of several successive refinement steps. The system should be compliant not only with the final specification, but also with all specifications in the chain of refinements. Consequently, we may need several notions of compliance corresponding to the various notions of refinement.

As a computer program or other system representation may be viewed as a specification, one might ask why compliance is not identical to refinement. The reason for defining compliance separately from refinement is that a system representation is (ideally) complete, while sequence diagrams are partial specifications. Sequence diagrams may include so-called implied scenarios, as explained under "Restricted compliance relation" in Section 4.2 of [RRS07]. Implied scenarios must be taken into account when defining compliance. For example, some refinement relations allow only behavior that is explicitly described as acceptable at the abstract level to be acceptable at the concrete level. If compliance was identical to refinement this would imply that specifications with implied scenarios could not be complied with, since the implied scenarios would occur explicitly in the system representation but not in the sequence diagram specification.

[3] Note that we use the term "constraint" rather loosely. For instance, the addition of a new constraint may result in the specification requiring more behaviours of the system.

In this paper we only consider compliance for probabilistic sequence diagrams without external input and output. For such sequence diagrams, we propose the following compliance checking procedure:

1. Given a computer system $I$ and a sequence diagram $d$, use e.g. testing on $I$ to obtain a probability space representing the system behavior, where the sample space is the set of all traces that may be produced by $I$.
2. Transform this probability space into the same semantic model as that used for $d$.
3. Depending on the kind of compliance desired, select the appropriate compliance relation.
4. $I$ is compliant with $d$ if this compliance relation holds between the semantics of $d$ and the representation of $I$ obtained in step 2.

In practice, a test will always give an imperfect picture of the system, since the test will necessarily be finite. Only a finite number of trace instances can be observed. Firstly, this means that the set of all observed traces may be only a subset of the traces that the system is actually able to produce. Secondly, since the probabilities obtained from a test will be based on frequencies of observed trace instances, the probabilities will necessarily be inaccurate. However, the accuracy of the obtained probabilities can always be increased by increasing the number of observed trace instances. Thirdly, even if a system is in principle able to produce infinitely long traces, we can only observe finite traces. In such cases the best we can do is to make an estimate based on the observed behaviour. For example, if the same output has been transmitted continuously for a long period of time, then we may assume that an infinite loop has been entered.

The above imperfections are unavoidable for any method of judging compliance based on testing, in contrast to methods based on full information about the internals of the system such as program code. But such information is usually too complex or not even accessible for those responsible for determining whether the system complies with the specification. Therefore a procedure based on testing is more useful in practice. It is up to those responsible for the test to decide how extensive the test should be, i.e. how many and how long observations should be made. This will depend on the nature of the system under consideration.

Different development stages may not only involve different notions of refinement and compliance, but also different requirements as regards probabilities. In early stages the focus may typically be on what alternatives the system should be able to produce, and developers will describe these alternatives until a suitable level of abstraction is reached. In these stages developers are not concerned with probability values. Therefore sequence diagrams with inherent nondeterminism, together with the appropriate refinement and compliance relations, offer a sufficient level of expressiveness. At a later stage it may be necessary to introduce probabilities for the different alternatives. To ensure that the intended relationships between specifications (or between specifications and system representations) are preserved when introducing probabilities two issues must be resolved. Firstly, a probabilistic interpretation of inherent nondeterminism must be established. Obviously, this interpretation must allow a large degree of freedom with respect to the actual probabilities; otherwise the developers would not be able to choose suitable probability values for the alternatives. Secondly, we need probabilistic counterparts to the refinement and compliance relations used for specifications with inherent nondeterminism. These relations should fulfill the following condition for all specifications of practical interest: If a certain relation holds for specifications with inherent nondeterminism then the probabilistic counterpart of this relation holds for the probabilistic interpretation of the specifications.

The rest of this paper is organized as follows: In Section 2 we state the requirements that a step-wise procedure for checking computer systems against probabilistic sequence diagrams needs to fulfill. The semantics of probabilistic STAIRS is explained in Section 3. Section 4 gives a number of alternative definitions of refinement. These definitions are evaluated and compared with respect to mathematical properties that are desirable from a practical point of view. Based on the refinement definitions given in Section 4 we define what it means for a system to be compliant with a probabilistic sequence diagram in Section 5. In Section 6 we give a probabilistic interpretation of sequence diagrams with inherent nondeterminism, and explore correspondence between refinement and compliance relations when switching from sequence diagrams with inherent nondeterminism to sequence diagrams with probabilistic choice, as discussed in the previous paragraph. We present some related work in Section 7 before concluding in Section 8.

Some new definitions and notations to facilitate formal proofs are introduced in Appendix A, while shorthand notation used in the proofs is explained in Appendix B. Finally, the proofs are contained in Appendix C.

## 2 Requirements

In order to motivate the following discussion and formal definitions, we formulate a number of requirements that our procedure has been designed to fulfill. That these requirements are met, is demonstrated throughout the discussion and summed up in Section 8.

1. The procedure should be independent of the choice of programming language in which the system is implemented. A sequence diagram does not prescribe any particular programming language, and the procedure should be sufficiently general to capture all possible choices. In general, we cannot assume that we have access to the source code of the system. This means that the only knowledge about the system that may be used by the procedure, is what can be obtained by testing. Although not feasible in practice, we assume that we are able to observe infinite runs. Otherwise, only safety properties could be falsified.
2. The notion of compliance should be a special case of refinement. Given a sequence diagram and its refinement, the procedure should give that a system

is compliant with the refinement only if the system is also compliant with the original sequence diagram.

3. The procedure should allow inherently nondeterministic choices in a specification to be replaced by probabilistic choices at some point in the development process. This allows developers to focus on specifying the relevant alternatives in the early stage of the process, and then add probabilities later. It should therefore be possible to interpret a specification with inherent nondeterminism as a probabilistic specification with a large degree of underspecification with respect to probabilities. The compliance and refinement relations used the for the specification with nondeterministic choice should have probabilistic counterparts such that for all practical specifications the relations are preserved when switching to the probabilistic interpretation.
4. The procedure should be faithful to the underlying ideas and principles of UML 2.1 [OMG06] sequence diagrams. UML is the leading specification language within the software industry of today, and our goal is that our approach should be of help for UML practitioners.

## 3 The semantics of probabilistic STAIRS

In this section we explain and define the semantics of pSTAIRS. We start by giving a thorough explanation of the operator palt for probabilistic choice.

### 3.1 Generalizing xalt into palt

Using xalt to specify inherent nondeterminism is not necessarily sufficient to capture the desired system behavior. Most likely, the owner of the gambling machine in Section 5.3 in [RRS07] wants it to be profitable. Hence, the chance of winning should be significantly less than the chance of losing.

In order to specify probabilities for each alternative, the palt operator (first introduced in [RHS05]) may be used instead of the xalt operator. The palt operator describes the probabilistic choice between two or more alternative operands whose joint probability should add up to one. Each operand is assigned a set of probabilities, and each operand should be chosen with a probability in its probability set. By using sets of probabilities instead of a single probability for each operand we allow underspecification with respect to probabilities. This allows us to specify for example a coin toss where any probability between 0.4 and 0.6 is acceptable for the two possible outcomes.

At the semantic level, interaction obligations are replaced by *p-obligations* of the form $((p,n),Q)$, where $(p,n)$ is an interaction obligation and $Q$ a set of allowed probabilities. A p-obligation $(o',Q')$ refines a p-obligation $(o,Q)$ if $o'$ refines $o$ and $Q' \subseteq Q$. For the time being we assume the notion of general refinement (defined on page 10 in [RRS07]) lifted from sets of interaction obligations to sets of p-obligations in the obvious way.

Probabilities other than 1 can only be introduced in a p-obligation by the palt operator. Any specification without a palt operator will contain exactly one p-obligation, and the probability set of this p-obligation will be $\{1\}$. The definition of the palt semantics is fairly complicated and involves some new operators on p-obligations and probability sets. We therefore introduce this definition in a stepwise manner. First we give three preliminary definitions and explain why these do not work as desired. The preliminary definitions are (3), (5) and (8). Then we present Definition (9), which is how the palt-semantics is defined. Definition (5) is a strengthening of (3), (8) is a strengthening of (5) and (9) is a strengthening of (8).

Before defining the semantics of the palt, we define the notion of probability decoration, which is used to assign probabilities to each operand of the palt operator. Probability decoration may only occur in the operands of a palt and is denoted by $d;Q$ in the textual syntax, where $d$ is a sequence diagram and $Q$ is a set of probabilities. Intuitively, $d;Q$ states that the operand $d$ should be selected with a probability in $Q$. Semantically, probability decoration is defined by:

$$[\![\ d;Q'\ ]\!] \overset{\mathsf{def}}{=} \{(o, Q * Q') \mid (o, Q) \in [\![\ d\ ]\!]\} \tag{1}$$

Multiplication of probability sets is defined by

$$Q_1 * Q_2 \overset{\mathsf{def}}{=} \{q_1 * q_2 \mid q_1 \in Q_1 \wedge q_2 \in Q_2\} \tag{2}$$

A diagram on the form $\mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)$ can be read as "one of the operands $d_1, \ldots, d_n$ should be selected; operand $d_1$ should be selected with a probability in $Q_1$ and ... and the operand $d_n$ should be selected with a probability in $Q_n$".

It would be intuitively tempting to define the palt semantics in a similar way as the xalt semantics, with the only difference being that each operand is assigned a probability set. This would give the following definition:

$$[\![\ \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)\ ]\!] \overset{\mathsf{pre}}{=} \bigcup_{j=1}^{n} [\![\ d_j;Q_j\ ]\!] \tag{3}$$

where we use $\overset{\mathsf{pre}}{=}$ to show that this is a preliminary definition. However, Definition 3 is not satisfactory. The reason is that we allow underspecification with respect to probabilities, but the definition does not ensure that the probabilities of the operands are chosen so that they add up to 1. To see this, assume we want to specify a coin toss with a coin that is not necessarily completely fair, so we accept any probability between 0.4 and 0.6 for the two alternatives, leaving the exact amount of unfairness open for the implementers to decide. The two acceptable outcomes are heads and tails, represented by the corresponding messages. It is not acceptable for the coin to come to rest standing on its side. We try to express this by the specification in Figure 1. In the graphical notation we write the probability sets for each operand to the palt operator after the operator name. The first probability set belongs to the first operator, the second probability set to the second operator, and so on. The operators alt and refuse are used to define the positive and the negative traces of the interaction obligations representing heads and tails. Formal definitions are given in Definition (15) and Definition (16) in Section 3.2. Now let

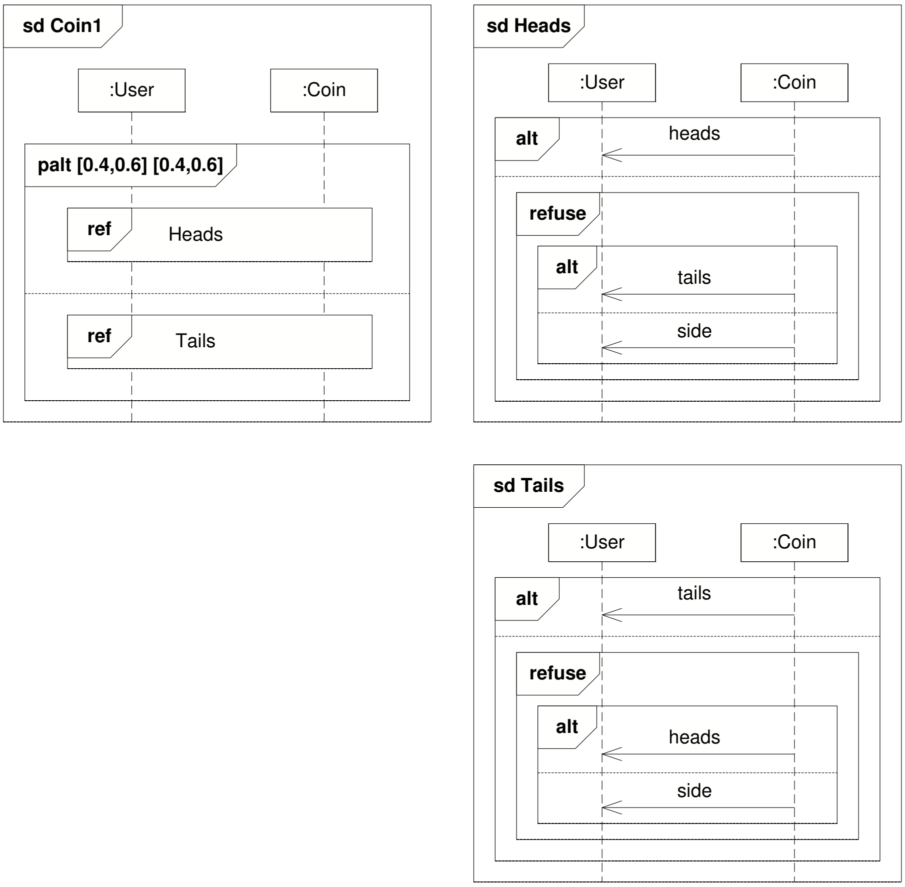

**Fig. 1.** A coin toss with underspecification with respect to probabilities

$$\begin{aligned}
s_h &= \{\langle !heads, ?heads\rangle\}\\
s_t &= \{\langle !tails, ?tails\rangle\}\\
s_s &= \{\langle !side, ?side\rangle\}\\
o_h &= (s_h, s_t \cup s_s)\\
o_t &= (s_t, s_h \cup s_s)
\end{aligned}$$

According to Definition (3) we then get

$$[\![ \text{ Coin1 } ]\!] = \{(o_h, [0.4, 0.6]), (o_t, [0.4, 0.6])\}.$$

But this does not ensure that if probability 0.4 is chosen for the heads alternative then probability 0.6 is chosen for the tails alternative, and Coin1 could be refined by a specification where the probability of both the heads and tails alternatives are 0.4 – which leaves room for behavior that is not acceptable in any of these alternatives. For example, the specification Coin2 in Figure 2 would be a valid refinement of Coin1, since $(o_h, [0.4, 0.6])$ would be refined by $(o_h, \{0.4\})$ and $(o_t, [0.4, 0.6])$ would be refined by $(o_t, \{0.4\})$. This was not intended, as Coin2 allows the coin to come to rest standing on its side with the probability of 0.2.

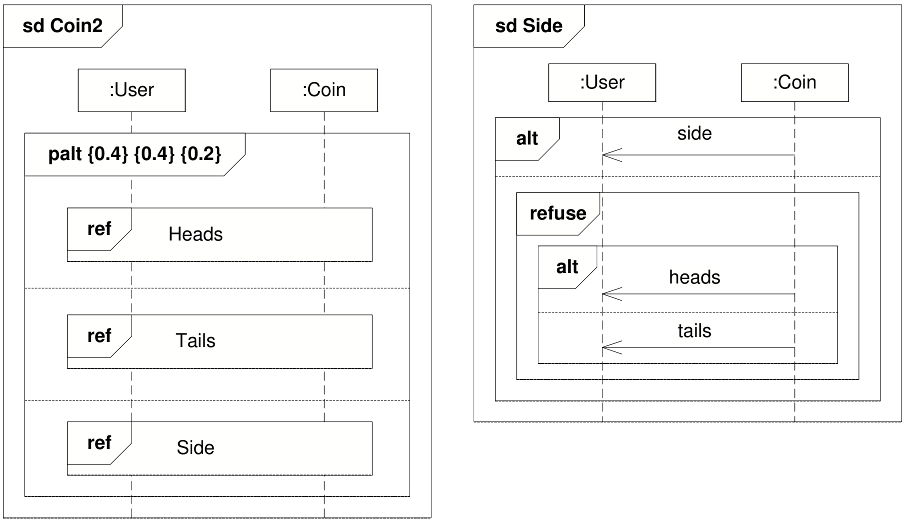

**Fig. 2.** A coin toss where the coin may come to rest standing on its side

To ensure that the chosen probabilities of the operands add up to 1 we strengthen the palt semantics with an additional p-obligation representing the combination of all the p-obligations we obtain from the operands. The only acceptable probability for this combined p-obligation is 1. This formalizes that one of the operands must be chosen; i.e. the probabilistic choice will be made among the specified operands. For the Coin1 specification this means that we add a p-obligation $(o_{ht}, \{1\})$ representing the combination of the heads and the tails alternatives. The positive and negative traces of $o_{ht}$ are determined by the interaction obligations of the original p-obligations $(o_h, [0.4, 0.6])$ and $(o_h, [0.4, 0.6])$. If a trace is positive in one of these then it is acceptable for the system to produce this trace. Therefore, if a trace is positive in at least one p-obligation (and not inconclusive in any p-obligation) then it is positive in the combined p-obligation. For the Coin1 specification this means that traces in $s_h \cup s_t$ are positive. If a trace is negative in all the original p-obligations then this means that it should not be produced at all. Hence it is also negative in the combined p-obligation. For the Coin1 specification this means that traces in $s_s$ are negative. If a trace is inconclusive in at least one of the original p-obligations then it has not been considered for all alternatives. It is therefore considered to be inconclusive also in the combined p-obligation. In the Coin1 specification the union of positive and negative traces is the same for all the p-obligations of the operands of palt – as discussed later we believe that from a practical point of view this is normally advisable.

The interaction obligation of the combined p-obligation is formalized by the $\oplus$ operator, whose operand is a set of p-obligations:

$$\oplus S \overset{\mathsf{def}}{=} ((\bigcup_{((p,n),Q)\in S} p) \cap (\bigcap_{((p,n),Q)\in S} p \cup n), \bigcap_{((p,n),Q)\in S} n) \qquad (4)$$

As explained above, a trace is negative only if it is negative in all p-obligations; a trace is inconclusive if it is inconclusive in at least one p-obligation, and positive otherwise. In the Coin1 specification the interaction obligation of the combined p-obligation is

$$o_{ht} = \oplus\{((s_h, s_t \cup s_s), [0.4, 0.6]), ((s_t, s_h \cup s_s), [0.4, 0.6])\} = (s_h \cup s_t, s_s)$$

To include the combined p-obligation in the palt semantics we add another line to the previous definition:

$$[\![ \ \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n) \ ]\!] \overset{\mathsf{pre}}{=} \qquad (5)$$

$$\bigcup_{j=1}^{n} [\![ \ d_j;Q_j \ ]\!] \ \cup \qquad (a)$$

$$\{(\oplus \bigcup_{j=1}^{n} [\![ \ d_j;Q_j \ ]\!], \{1\})\} \qquad (b)$$

Note that line (b) in Definition (5) implies that nesting of palt operators is significant. This means that a specification with nested palt cannot in general be rewritten into an equivalent specification with only a single palt operator. As an example, consider the specifications Nested and Flat in Figure 3. The specifications are represented as interaction overview diagrams with probability decorations for each palt-operand. Specification Nested is stricter than Flat,

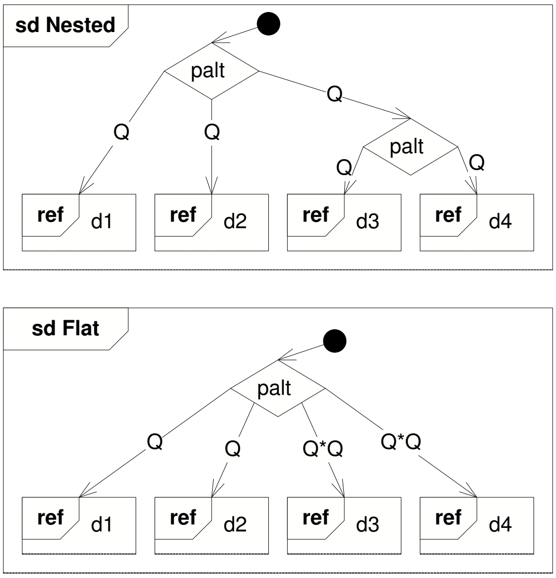

**Fig. 3.** Specification Nested is stricter than specification Flat

because Nested requires that the probability of selecting one of d3 and d4 is a value in $Q$. This is not required by Flat. For example, let $Q = [\frac{1}{4}, \frac{1}{2}]$, which gives $Q * Q = [\frac{1}{16}, \frac{1}{4}]$. According to Flat it would be acceptable to select d1 with probability $\frac{1}{2}$, d2 with probability $\frac{3}{8}$, d3 with probability $\frac{1}{16}$ and d4 with probability $\frac{1}{16}$. According to Nested this is not acceptable, since the probability of selecting one of d3 and d4 is then $\frac{1}{8}$, which is not a value in $[\frac{1}{4}, \frac{1}{2}]$. This illustrates the extra expressiveness obtained by including line (b) in Definition 5.

But Definition 5 is also unsatisfactory. The reason is that it allows more than one p-obligation at the abstract level to be represented by the same p-obligation at the concrete level. To see this we look at an example where a palt operator has more than two operands. Assume we want to specify a system that simulates a player of the game Rock, Scissors, Papers. The system must be able to produce traces representing each of the outcomes rock, scissors and paper, and we allow the probability of each of these alternatives to be between $\frac{1}{4}$ and $\frac{1}{2}$. This is specified by the diagram Rsp1 in Figure 4. Intuitively, it is clear that the Rsp1 specification should not allow the trace $\langle !rock, ?rock \rangle$ to be produced with a probability higher than $\frac{1}{2}$, since this trace is negative both in the p-obligation representing scissors and the p-obligation representing paper. Since each of these two p-obligations have a lowest acceptable probability of $\frac{1}{4}$, this specification should ensure that the trace $\langle !rock, ?rock \rangle$ is not produced with a probability higher than $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. But this is not ensured; we may circumvent this intuitive requirement by letting the three p-obligations in $[\![$ Rsp1 $]\!]$ representing rock, scissors and paper be refined by one and the same p-obligation at the concrete

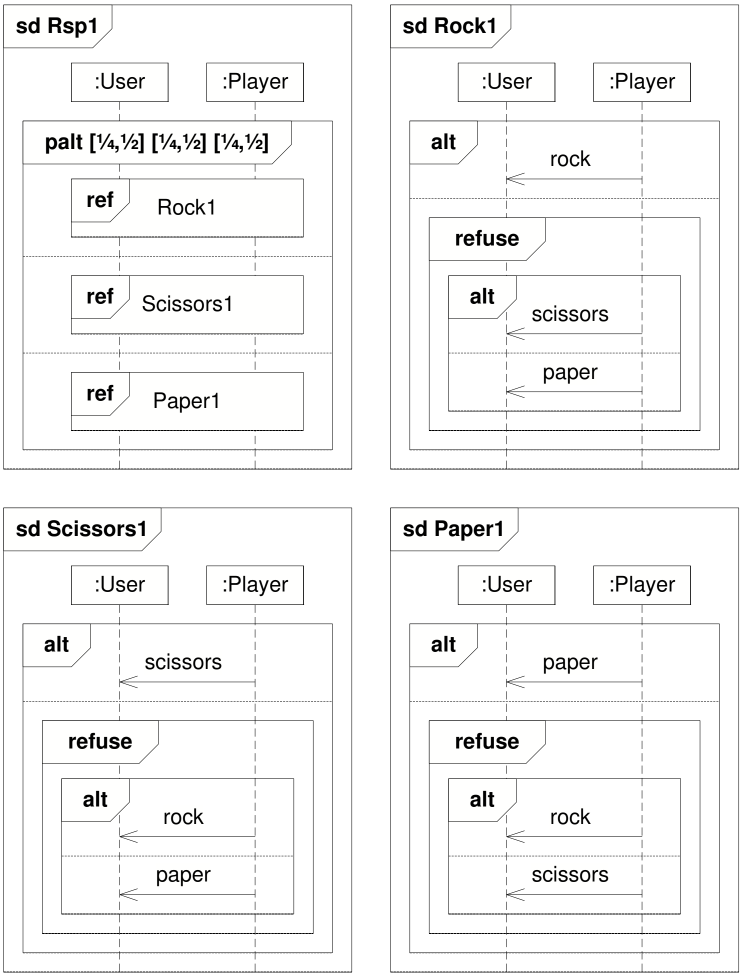

**Fig. 4.** Rock, Scissors, Paper

level, while at the same time adding two additional p-obligations that refine only the p-obligation representing rock. This is illustrated by the specification Rsp2 in Figure 5. Figure 6 shows how Rsp1 is refined by Rsp2. The upper row represents $[\![$ Rsp1 $]\!]$ and the lower row represents $[\![$ Rsp2 $]\!]$. Each p-obligation is illustrated by a circle representing the interaction obligation and a probability set. The upper part of the circle contains the positive traces and the lower part contains the negative traces. We have used the following trace names: $r = \langle !rock, ?rock\rangle$, $s = \langle !scissors, ?scissors\rangle$, $p = \langle !paper, ?paper\rangle$ and $t = \langle !twine, ?twine\rangle$. The rightmost p-obligations are those we get from line (b) in Definition (5). The arrows indicate the refinement relation between p-obligations. Rsp1 is refined by Rsp2 since each p-obligation in $[\![$ Rsp1 $]\!]$ is refined by at least one p-obligation in $[\![$ Rsp2 $]\!]$. But according to Rsp2, the trace $r$ may well occur with a probability greater than $\frac{1}{2}$, since it is allowed by all the p-obligations of $[\![$ Rsp2 $]\!]$ except number 2 from the left.

To avoid the above situation we strengthen the semantics of $\mathsf{palt}$ with p-obligations representing the combined sum of *any subset* of p-obligations from the original specification. For example, we include a p-obligation representing the combined sum of the rock outcome and the scissors outcome, i.e. a p-obligation where both these outcomes are possible. As before, the interaction obligation of a combined p-obligation is produced by the $\oplus$ operator. But since each new combination represents only a subset of the original p-obligations, we cannot use 1 as the only acceptable probability. Instead we use the sum of the probability sets of each p-obligation of the subset. The combined sum operator $\bar{\oplus}$ combines an indexed set $\{(o_i, Q_i)\}_{i\in N}$ of p-obligations into a single p-obligation as follows:

$$\bar{\oplus}(\{(o_i, Q_i)\}_{i\in N}) \overset{\mathsf{def}}{=} (\oplus\{(o_i, Q_i) \mid i \in N\}, \sum_{i\in N} Q_i) \tag{6}$$

Summation of probability sets is done by choosing one value from each set and then adding those combinations that do not exceed 1. Formally, summation of $n$ probability sets is defined by:

$$\sum_{i=1}^{n} Q_i \overset{\mathsf{def}}{=} \{\mathsf{min}(\sum_{j=1}^{n} q_j, 1) \mid \forall j : q_j \in Q_j\} \tag{7}$$

Note that $\bar{\oplus}\{(o, Q)\} = (o, Q)$ for any $Q \subseteq [0, 1]$.

The following definition of $\mathsf{palt}$, in which line (a) in Definition (5) has been replaced, ensures that all possible combinations of p-obligations coming from the operands of the $\mathsf{palt}$ are included:

$$[\![\ \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)\ ]\!] \overset{\mathsf{pre}}{=} \tag{8}$$

$$\{\bar{\oplus}(\{po_i\}_{i\in N}) \mid N \subseteq \{1, \ldots, n\} \wedge N \neq \emptyset \wedge \forall i \in N : po_i \in [\![\ d_i;Q_i\ ]\!]\} \cup \quad \text{(a)}$$

$$\{(\oplus \bigcup_{j=1}^{n} [\![\ d_j;Q_j\ ]\!], \{1\})\} \quad \text{(b)}$$

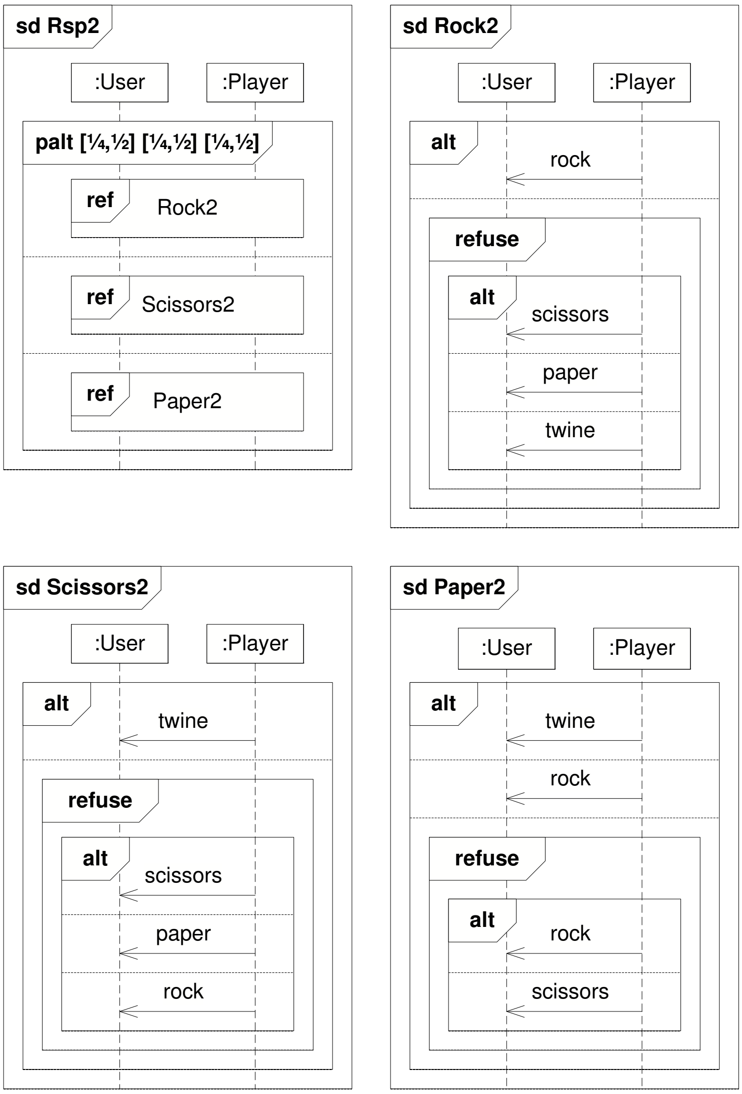

**Fig. 5.** An undesired refinement of Rock, Scissors, Paper

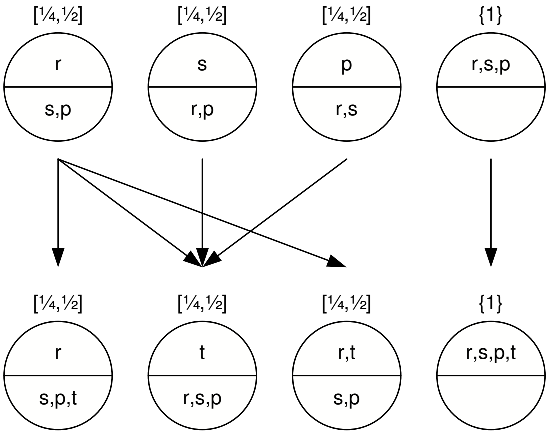

**Fig. 6.** Rsp1 is refined by Rsp2

Note that the set of p-obligations we get from (8a) is a superset of the set we get from (5a).

Figure 7 illustrates the semantics and refinement relations of Rsp1 and Rsp2 when Definition (8) is applied. With this definition it is clear that Rsp2 is not a refinement of Rsp1, since one of the p-obligation in $[\![$ Rsp1 $]\!]$ (the one representing the combination of the scissors and paper outcomes) is not refined by any p-obligation from $[\![$ Rsp2 $]\!]$.

The vertical dotted lines in Figure 7 illustrate from which part of Definition (8) the p-obligations come. For the p-obligations coming from (8a) we have indicated the number of p-obligations that have been combined by $\#N = x$ for $x \in \{1, 2, 3\}$. Note that the set of p-obligations we get from Definition (5) is a subset of the set we get from Definition (8). This is because $po = \bar{\oplus}\{po\}$ for any p-obligation $po$.

The p-obligations illustrated by dotted circles in Figure 7 are repetitions of p-obligations that are already in the set. They have been included to make it easier to understand how the palt semantics is calculated.

Note that Definition (8) implies that a single palt operand at the abstract level may be split into several operands in a refinement. Consider the specifications Rsp3 og Rsp4 in Figure 8. The only difference between these two specifications is the following: Rsp3 requires that the rock and/or scissors outcomes are produced with a probability of $\frac{2}{3}$, but it does not say anything about the internal distribution between these outcomes. Rsp4, on the other hand, requires that the probability of producing each of the outcomes rock and scissors is $\frac{1}{3}$. Clearly, this is a stricter requirement that implies the requirement from Rsp3. Therefore Rsp4 should be a refinement of Rsp3. However, if we used Definition (5) instead of Definition (8), then this would not be the case. To see this, note that $[\![$ Rsp3 $]\!]$ includes the p-obligation $((\{r, s\}, \{p\}), \{\frac{2}{3}\})$, whether we use Definition (5) or

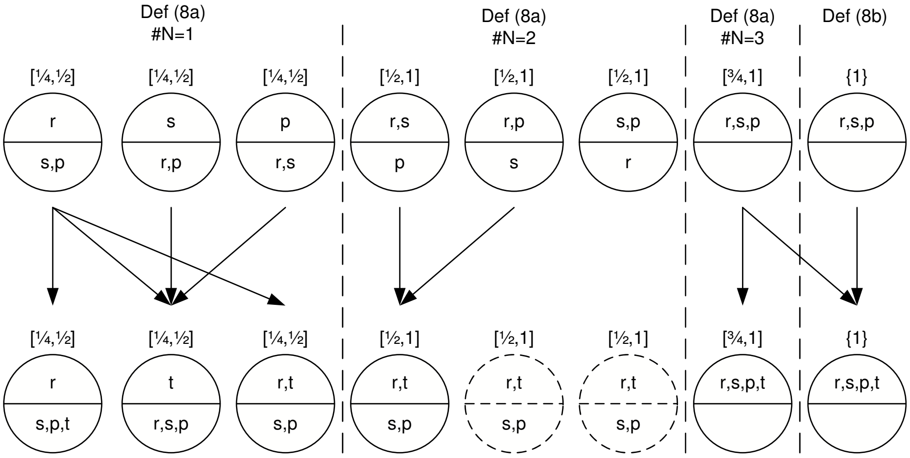

**Fig. 7.** With Definition (8), Rsp1 is *not* refined by Rsp2

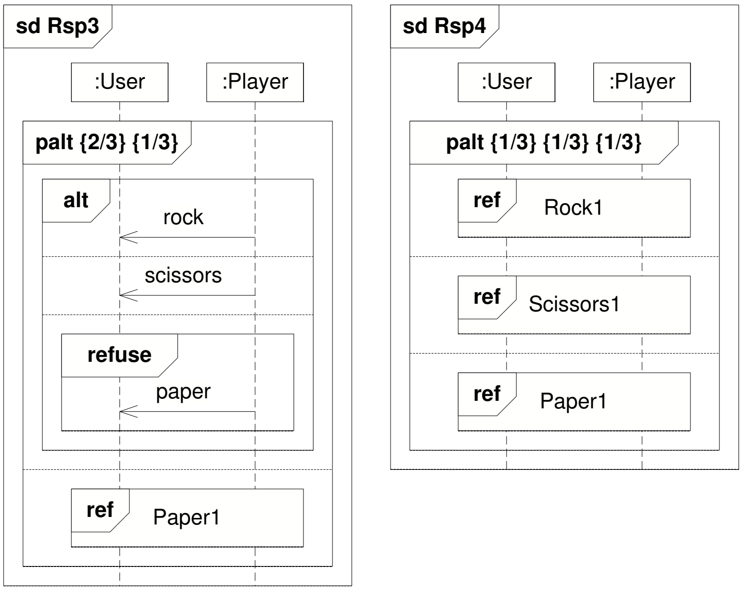

**Fig. 8.** Splitting of palt operands

Definition (8). This p-obligation need to be refined by a p-obligation in $[\![$ Rsp4 $]\!]$. But if we use Definition (5) then $[\![$ Rsp4 $]\!]$ will not contain any p-obligation with probability set $\{\frac{2}{3}\}$, so the refinement relation does not hold. On the other hand, using Definition (8) we get a p-obligation representing the combined sum of the rock and the scissors alternatives (from the first and second $\mathsf{palt}$-operands of Rsp4). This combined sum is identical to $((\{r, s\}, \{p\}), \{\frac{2}{3}\})$, so it follows that each p-obligation in $[\![$ Rsp3 $]\!]$ is refined by a p-obligation in $[\![$ Rsp4 $]\!]$.

One last consideration has to be made before we give the final definition of $\mathsf{palt}$. This consideration regards the p-obligation representing the combination of all other p-obligations that we introduced in Definition 5. The $\mathsf{palt}$ operator is meant to represent a complete probabilistic choice in the sense that the sum of the probabilities chosen for each operand should not be less than 1. If this cannot be achieved then no system should comply with the specification. We ensure this by substituting $\{1\}$ with $\{1\} \cap \sum_{j=1}^{n} Q_j$ in (8b). This gives us the following definition:

$$[\![\ \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)\ ]\!] \overset{\mathsf{def}}{=} \tag{9}$$

$$\{\bar{\oplus}(\{po_i\}_{i \in N}) \mid N \subseteq \{1, \ldots, n\} \wedge N \neq \emptyset \wedge \forall i \in N : po_i \in [\![\ d_i;Q_i\ ]\!]\} \cup \tag{a}$$

$$\{(\oplus \bigcup_{i=1}^{n} [\![\ d_i;Q_i\ ]\!], \{1\} \cap \sum_{j=1}^{n} Q_j)\} \tag{b}$$

As explained further in Section 5, no system can comply with a specification whose semantics contains a p-obligation with an empty probability set.

Note that, due to Definition (7), Definition (9b) means that $\{1\} \cap \sum_{i=1}^{n} Q_i$ will be equal to $\{1\}$ even if all possible choices of one probability from each probability set $Q_i$ gives a sum that is greater than 1. This means that it may be possible to comply with such a specification, as long as the operands of the $\mathsf{palt}$ is overlapping in the sense that there exists a behavior that is allowed by more than one operand. For example, assuming it is possible to comply with the specification $d$, then it is also possible to comply with the specification $\mathsf{palt}(d;\{1\}, d;\{1\})$[4].

### 3.2 Generalizing the other operators

$\mathcal{E}$ denotes the set of all events. The semantics of an event $e \in \mathcal{E}$ is generalized by assigning 1 as the only allowed probability:

$$[\![\ e\ ]\!] \overset{\mathsf{def}}{=} \{((\langle e \rangle, \emptyset), \{1\})\} \tag{10}$$

[4] Another example is the following case: assume that $[\![\ d_1\ ]\!]$ contains a single p-obligation that according to the chosen compliance relation allows any traces except $t_1$. Similarly, assume that $[\![\ d_2\ ]\!]$ allows any traces except $t_2$. Assume furthermore that $I$ is a system that produces the trace $t_1$ with probability 0.4, $t_2$ with probability 0.3, and $t_3$ with probability 0.3. From Section 5 it will be clear that $I$ complies with the specification $\mathsf{palt}(d_1;\{0.6\}, d_2;\{0.7\})$, partly because the trace $t_3$ is allowed by both $d_1$ and $d_2$.

Before giving the generalized semantics of $\mathsf{seq}$, $\mathsf{par}$, $\mathsf{alt}$ and $\mathsf{refuse}$ we need to extend the definitions of the semantical composition operators to sets of p-obligations. The composition of two sets of p-obligations is the set we may obtain by choosing one p-obligation from each set and composing these two p-obligations. Since these choices are made independently from each other, probability sets are multiplied. Hence, parallel composition ($\|$), sequential composition ($\succsim$), underspecification ($\uplus$) and refusal ($\dagger$) carry over from sets of interaction obligations to sets of p-obligations in a straightforward manner:

$$\begin{aligned} O_1 \; op \; O_2 &\overset{\mathsf{def}}{=} \{(o_1 \; op \; o_2, Q_1 * Q_2) \mid \\ &\qquad (o_1, Q_1) \in O_1 \wedge (o_2, Q_2) \in O_2\} \end{aligned} \tag{11}$$

$$\dagger O_1 \overset{\mathsf{def}}{=} \{(\dagger o_1, Q_1) \mid (o_1, Q_1) \in O_1\} \tag{12}$$

where $op$ is one of $\|$, $\succsim$ and $\uplus$. We may then define $\mathsf{seq}$, $\mathsf{par}$, $\mathsf{alt}$ and $\mathsf{refuse}$ as follows:

$$\llbracket\; d_1 \;\mathsf{par}\; d_2 \;\rrbracket \overset{\mathsf{def}}{=} \llbracket\; d_1 \;\rrbracket \,\|\, \llbracket\; d_2 \;\rrbracket \tag{13}$$

$$\llbracket\; d_1 \;\mathsf{seq}\; d_2 \;\rrbracket \overset{\mathsf{def}}{=} \llbracket\; d_1 \;\rrbracket \succsim \llbracket\; d_2 \;\rrbracket \tag{14}$$

$$\llbracket\; d_1 \;\mathsf{alt}\; d_2 \;\rrbracket \overset{\mathsf{def}}{=} \llbracket\; d_1 \;\rrbracket \uplus \llbracket\; d_2 \;\rrbracket \tag{15}$$

$$\llbracket\; \mathsf{refuse}\; d \;\rrbracket \overset{\mathsf{def}}{=} \dagger\llbracket\; d \;\rrbracket \tag{16}$$

As in [RRS07] we also introduce the macro operator $\mathsf{veto}$ defined by:

$$\mathsf{veto}\; d \overset{\mathsf{def}}{=} \mathsf{skip\ alt\ refuse}\; d \tag{17}$$

where

$$\llbracket\; \mathsf{skip} \;\rrbracket \overset{\mathsf{def}}{=} \{((\{\langle\rangle\}, \emptyset), \{1\})\} \tag{18}$$

Notice that in all the examples the p-obligations of the different $\mathsf{palt}$-operands have the same set of inconclusive traces. For practical specifications we believe that this should normally be the case. Specifying probabilistic alternatives does not make much sense unless they are mutually exclusive in the sense that the positive traces in one operand are negative in the other. Consider again the specification of a coin toss. If traces representing heads are inconclusive in the tails alternative then they can in a refinement be introduced as positive in the tails alternative, which is obviously not the intention behind the specification. Actually, for practical purposes we believe the following macro operator for ensuring mutual exclusion is useful:

$$\begin{aligned} &\llbracket\; \mathsf{expalt}(d_1;Q_1, \ldots, d_n;Q_n) \;\rrbracket \overset{\mathsf{def}}{=} \\ &\quad \llbracket\; \mathsf{palt}((d_1 \;\mathsf{alt\ refuse}(d_2 \;\mathsf{alt}\; \ldots \;\mathsf{alt}\; d_n));Q_1, \\ &\qquad\quad \ldots \\ &\qquad\quad (d_n \;\mathsf{alt\ refuse}(d_1 \;\mathsf{alt}\; \ldots \;\mathsf{alt}\; d_{n-1}));Q_n) \;\rrbracket \end{aligned} \tag{19}$$

# 4 Refinement

Refinement means to add more information to the specification in order to bring it closer to a real system. When performing a series of refinement steps it is important that the end result refines the original specification. Since practical specifications may be quite large, it is also important that different parts of a sequence diagram may be refined separately. In this section we present a number of refinement relations and evaluate these against the above criteria.

In [RRS07] two basic refinement relations $\rightsquigarrow_r$ and $\rightsquigarrow_{rr}$ are defined at the semantic level. They characterize what it means for one interaction obligation to refine another interaction obligation. These two basic definitions are then used to define the various refinement and compliance relations at the syntactic level (i.e. at the level of specifications expressed as sequence diagrams). Furthermore, the syntactic relations are investigated formally with respect to desirable properties. In this paper we follow a similar strategy, with the exception that we operate with three basic relations, not just two as in the non-probabilistic case. The third basic relation ($\rightsquigarrow_{nr}$) is introduced as an alternative to the $\rightsquigarrow_{rr}$ relation.

## 4.1 Refinement relations for single interaction obligations

The refinement relations $\rightsquigarrow_r$, $\rightsquigarrow_{rr}$ and $\rightsquigarrow_{nr}$ are defined as follows:

$$(p, n) \rightsquigarrow_r (p', n) \overset{\mathsf{def}}{=} n \subseteq n' \land p \subseteq p' \cup n' \tag{20}$$

$$(p, n) \rightsquigarrow_{rr} (p', n) \overset{\mathsf{def}}{=} (p, n) \rightsquigarrow_r (p', n') \land p' \subseteq p \tag{21}$$

$$(p, n) \rightsquigarrow_{nr} (p', n') \overset{\mathsf{def}}{=} (p, n) \rightsquigarrow_r (p', n') \land p \cup n = p' \cup n' \tag{22}$$

As explained in [RRS07], the refinement relation $\rightsquigarrow_r$ allows the incompleteness of a specification to be reduced by introducing more positive and/or negative behaviors to the specification, and hence reduce the set of inconclusive traces. In addition, underspecification may also be reduced by redefining positive traces as negative.

At some stage in the development process it may be natural to fix the set of positive traces, with the intention that at least one of these traces should be present in a system compliant with the specification. A valid refinement step may therefore only redefine positive and inconclusive traces as negative, while extending the set of positive traces is not allowed. This is represented by the refinement relation $\rightsquigarrow_{rr}$. The idea is that refinement relations based on $\rightsquigarrow_r$ and $\rightsquigarrow_{rr}$ will be used in different phases of the development process.

However, as will be clear from Section 4.5, there are certain desirable properties that the refinement relations based on $\rightsquigarrow_{rr}$ do not fulfill in the probabilistic case. We have therefore introduced a third refinement relation $\rightsquigarrow_{nr}$ for interaction obligations, where the $n$ stands for narrowing. This relation is intended as an alternative to $\rightsquigarrow_{rr}$ for probabilistic specifications. It will be shown that refinement relations based on $\rightsquigarrow_{nr}$ fulfill the desirable properties also in the probabilistic case. The intuitive motivation for narrowing refinement is quite similar to that of restricted refinement. During the specification process we may reach a point where all behavior we consider to be relevant and interesting has been described. This includes normal behavior, exceptional behavior and erroneous behavior. At this point we may decide that supplementing (introducing new traces) is no longer allowed, which is ensured by the right-hand conjunct of (22). However, some design decisions may still be open. Hence, the specification may include underspecification in form of positive behavior that need not occur in a valid implementation.

The essential difference between $\rightsquigarrow_{rr}$ and $\rightsquigarrow_{nr}$ is that $\rightsquigarrow_{rr}$ allows inconclusive traces to be redefined as negative. This is not allowed by $\rightsquigarrow_{nr}$. Refinement relations based on $\rightsquigarrow_{nr}$ should therefore only be used after all relevant and interesting behavior (including negative behavior) has been identified.

### 4.2 Refinement relations for single p-obligations

A p-obligation is refined by refining its interaction obligation and/or reducing its set of allowed probabilities. The interaction obligation may be refined either by $\rightsquigarrow_r$, $\rightsquigarrow_{rr}$ or $\rightsquigarrow_{nr}$:

$$(o, Q) \rightsquigarrow_{px} (o', Q') \overset{\mathsf{def}}{=} o \rightsquigarrow_x o' \wedge Q' \subseteq Q \tag{23}$$

where $x \in \{r, rr, nr\}$.

### 4.3 General, restricted general and narrowing general refinement

General refinement of specifications is defined for each of the three variants of refinement of a single p-obligation:

$$\begin{aligned} &[\![\ d\ ]\!] \rightsquigarrow_x [\![\ d'\ ]\!] \overset{\mathsf{def}}{=} \\ &\forall po \in [\![\ d\ ]\!] : 0 \notin \pi_2.po \Rightarrow \exists po' \in [\![\ d'\ ]\!] : po \rightsquigarrow_y po' \end{aligned} \tag{24}$$

where $(x, y) \in \{(pg, pr), (prg, prr), (png, pnr)\}$. Apart from the antecedent allowing p-obligations with 0 as an acceptable probability to be ignored, the considerations regarding refinement of probabilistic sequence diagrams are exactly the same as for sequence diagrams with inherent nondeterminism. The antecedent is neccessary to allow a proper treatment of soft real-time requirements, which are requirements such as “after event A has occurred, event B should occur within 5 seconds with a probability of at least 0.9”. A system that always produces event B within 5 seconds of producing event A would certainly comply with this requirement. We enable expression of soft real-time requirements by allowing that p-obligations with 0 as an acceptable probability are not represented at the concrete level. A soft real-time requirement can then be expressed with a palt operator with two operands: one for the case where event B occurs within 5 seconds, and another where it does not. This latter operand will have 0 as one of its acceptable probabilities. For simplicity time constraints have not been included in this report. For more on specifications with soft real-time requirements, see [RHS07a].

### 4.4 Limited, restricted limited and narrowing limited refinement

Limited refinement of specifications is defined for each of the three variants of refinement of a single p-obligation:

$$\begin{aligned} & [\![\, d \,]\!] \leadsto_x [\![\, d' \,]\!] \overset{\mathsf{def}}{=} \\ & \quad [\![\, d \,]\!] \leadsto_y [\![\, d' \,]\!] \wedge \\ & \quad \forall po' \in [\![\, d' \,]\!] : \exists S \subseteq [\![\, d' \,]\!] : \exists po \in [\![\, d \,]\!] : po' \in S \wedge po \leadsto_z \bar{\oplus} S \end{aligned} \tag{25}$$

where $(x, y, z) \in \{(pl, pg, pr), (prl, prg, prr), (pnl, png, pnr)\}$.

The additional requirement for limited refinement is intuitively that each p-obligation at the concrete level represents a p-obligation at the abstract level. However, it is perfectly acceptable to split a p-obligation at the abstract level into several p-obligations at the concrete level. For example, if $(o, \{0.5\})$ is a p-obligation of the abstract level, then this may be represented by the combination of $(o'_1, \{0.3\})$ and $(o'_2, \{0.2\})$ at the concrete level, where both $o'_1$ and $o'_2$ are refinements of $o$. This means that these two p-obligations are not valid refinements of any p-obligation at the abstract level, since $\{0.3\}$ and $\{0.2\}$ are not subsets of $\{0.5\}$. However, the combination $\bar{\oplus}\{(o'_1, \{0.3\}), (o'_2, \{0.2\})\}$ is a refinement of $(o, \{0.5\})$. Therefore the additional requirement for limited refinement is that each p-obligation at the concrete level is a member of a set whose combination is a refinement of an abstract p-obligation.

### 4.5 Transitivity and monotonicity

In this section we present results concerning transitivity and monotonicity for the refinement relations.

A refinement relation $\leadsto$ is transitive if the following holds: If $d_1$ is refined by $d_2$ and $d_2$ is refined by $d_3$, then $d_1$ is refined by $d_3$. Formally:

$$[\![\, d_1 \,]\!] \leadsto [\![\, d_2 \,]\!] \wedge [\![\, d_2 \,]\!] \leadsto [\![\, d_3 \,]\!] \Rightarrow [\![\, d_1 \,]\!] \leadsto [\![\, d_3 \,]\!] \tag{26}$$

Transitivity of refinement is important since it ensures that the result of successive refinement steps is a valid refinement of the original sequence diagram. The following table summarizes results with respect to transitivity. "Y" (for "Yes") in a cell indicates that the refinement relation is transitive, while "N" (for "No") indicates that it is not. In addition, each cell contains a reference to the relevant theorem. We write Tx for Theorem x in the table. The theorems can be found in Appendix C along with their proofs.

| $\leadsto_{pg}$ | $\leadsto_{prg}$ | $\leadsto_{pl}$ | $\leadsto_{prl}$ | $\leadsto_{png}$ | $\leadsto_{pnl}$ |
|---|---|---|---|---|---|
| Y: T1 in [RHS07a] | Y: T11 | Y: T12 | N: T13 | Y: T14 | Y: T15 |

A binary operator *op* is monotonic with respect to refinement if the following holds: If $d_1$ is refined by $d'_1$ and $d_2$ is refined by $d'_2$ then $d_1$ *op* $d_2$ is refined by $d'_1$ *op* $d'_2$. Formally:

$$[\![\, d_1 \,]\!] \leadsto [\![\, d'_1 \,]\!] \wedge [\![\, d_2 \,]\!] \leadsto [\![\, d'_2 \,]\!] \Rightarrow [\![\, d_1 \; op \; d_2 \,]\!] \leadsto [\![\, d'_1 \; op \; d'_2 \,]\!] \tag{27}$$

Monotonicity ensures that different parts of a sequence diagram may be refined separately. The following table summarizes results with respect to monotonicity of operators for different refinement relations.

| Operator | $\rightsquigarrow_{pg}$ | $\rightsquigarrow_{prg}$ | $\rightsquigarrow_{pl}$ | $\rightsquigarrow_{prl}$ | $\rightsquigarrow_{png}$ | $\rightsquigarrow_{pnl}$ |
|---|---|---|---|---|---|---|
| refuse | Y: T21 | Y: T23 | Y: T28 | Y: T33 | Y: T38 | Y: T43 |
| seq | Y: T3 in [RHS07a] | Y: T24 | Y: T29 | N: T34 | Y: T39 | Y: T44 |
| par | Y: T4 in [RHS07a] | Y: T25 | Y: T30 | N: T35 | Y: T40 | Y: T45 |
| alt | Y: T5 in [RHS07a] | Y: T26 | Y: T31 | N: T36 | Y: T41 | Y: T46 |
| palt | N: T22 | N: T27 | Y: T32 | N: T37 | N: T42 | Y: T47 |

From the evaluation summarized in the above tables we identify two "winners" among the proposed refinement relations; $\rightsquigarrow_{pl}$ and $\rightsquigarrow_{pnl}$ are the only refinement relations that fulfill all desired properties with respect to transitivity and monotonicity of all composition operators.

None of the general refinement relations ($\rightsquigarrow_{pg}$, $\rightsquigarrow_{prg}$ and $\rightsquigarrow_{png}$) gives monotonicity for palt[5]. Intuitively, the reason is that the definition of the semantics for each operator ensures that there is always a p-obligation with 1 as the only acceptable probability, see in particular (9b). This p-obligation restricts *all* behavior of a valid system, which means that new behavior that does not refine existing alternatives cannot be added. Therefore STAIRS may be more suitable than pSTAIRS at an early stage of the development process where not all alternatives have been identified.

The tables show that $\rightsquigarrow_{prl}$ does not fulfill the desired transitivity and monotonicity properties. This suggests that $\rightsquigarrow_{pnl}$ should be used instead of $\rightsquigarrow_{prl}$ for probabilistic specifications.

# 5 Compliance

In this section we define what it means for a system to be compliant with a probabilistic sequence diagram. To do this we need 1) a mathematical representation of the computer system, and 2) a characterization of the relation between a specification and the mathematical representation of the system.

## 5.1 Representation of a system

In the non-probabilistic case [RRS07] we assume that we know the set $traces(I)$ that the system $I$ is able to produce. In the probabilistic case we need in addition information about probabilities. The basic mathematical model of a probabilistic process is a probability space [Sko05],[Bré94]. A probability space is a triple $(\Omega, \mathcal{F}, f)$ where

– $\Omega$ is a *sample space*, i.e. a set of outcomes.

[5] The extra criteria given in [RHS07a] to ensure monotonicity with respect to palt for $\rightsquigarrow_{prg}$ is basically similar to limited refinement.

- $\mathcal{F}$ is a *σ-field* on $\Omega$, i.e. a set of subsets of $\Omega$ that is closed under complement and countable union, and that contains $\Omega$.
- $f$ is a *probability measure* on $\mathcal{F}$, i.e. a function from $\mathcal{F}$ to $[0, 1]$ assigning probabilities to the sets in $\mathcal{F}$ such that $f(\Omega) = 1$ and for any sequence $\omega_1, \omega_2, \ldots$ of disjoint sets from $\mathcal{F}$, the following holds: $f(\bigcup_{i=1}^{\infty} \omega_i) = \sum_{i=1}^{\infty} f(\omega_i)$.

To ensure that information about probabilities are included in the representation of the system $I$, we assume that $I$ is represented by a probability space $(traces(I), \mathcal{F}_I, f_I)$. (This means that $traces(I)$ is the sample space of this probability space.)

Clearly, we are not interested in an arbitrary $\mathcal{F}_I$. We need to ensure that the probability space gives the necessary information with respect to probabilities. $\mathcal{F}_I$ contains all sets for which the probability is known, and we could for example let $\mathcal{F}_I$ be the σ-field $\{\emptyset, traces(I)\}$. But a probability space with this σ-field would tell us nothing about probabilities, except that the probability of producing a trace in $traces(I)$ is 1. To ensure that the necessary information about probabilities is contained in the probability space we require $\mathcal{F}_I$ to be the *cone-σ-field* of $traces(I)$.

The cone-σ-field is the smallest σ-field [Dud02, p. 86] generated from the set $C_I$ of *cones* we obtain from $traces(I)$. The cone $c_t$ of a finite trace $t$ is the set of all traces with $t$ as a prefix, formally defined by:

$$c_t \overset{\mathsf{def}}{=} \{t' \in traces(I) \mid t \sqsubseteq t'\} \tag{28}$$

The set of cones $C_I$ contains the cone of every finite trace that is a prefix of a trace in $traces(I)$, formally defined by:

$$C_I \overset{\mathsf{def}}{=} \{c_t \mid \#t \in \mathbb{N}_0 \land \exists t' \in traces(I) : t \sqsubseteq t'\} \tag{29}$$

One may ask why we did not simply require $\mathcal{F}_I$ to be the power set of $traces(I)$. This would ensure that a representation of a system would contain information about the probability of *every* subset of $traces(I)$. The answer is that not all processes can be represented by a probability space whose σ-field is the power set of its sample space. For example, assume $I$ is a process that flips a fair coin infinitely many times. Then the set $traces(I)$ is uncountable, and the probability of each single trace is 0. According to the continuum hypothesis – which states that there is no set whose size is strictly between that of the integers and that of the real numbers – the cardinality of $traces(I)$ then equals the cardinality of the real numbers, and hence of $[0, 1]$. The following theorem taken from [Dud02, Appendix C] by Banach and Kuratowski then implies that there is no measure $f_I$ on $\mathbb{P}(traces(I))$ such that $f_I(\{t\}) = 0$ for each $t \in traces(I)$ and $f_I(traces(I)) = 1$:

> Assuming the continuum hypothesis, there is no measure $\mu$ defined on all subsets of $\Omega = [0, 1]$ with $\mu(\Omega) = 1$ and $\mu(x) = 0$ for each $x \in \Omega$.

Our decision to use a cone-based probability space to represent probabilistic systems is inspired by [Seg95]. In [Seg95, p. 52] probability spaces whose σ-fields are cone-σ-fields are used to represent fully probabilistic automata, i.e.

automata with probabilistic choice but without nondeterminism. This is done in order to define formally how to compute probabilities for trace sets. A cone-based probability space is a suitable representation of a probabilistic system, since it gives maximum information about probabilities while still allowing processes such as an infinite coin toss to be represented.

Note that for any trace $t$ in $traces(I)$ we have $\{t\} \in \mathcal{F}_I$ (which is proved in Lemma 27, Appendix C). As $\mathcal{F}_I$ is closed under countable union, this means that for any countable $s \subseteq traces(I)$ we have $s \in \mathcal{F}_I$. Consequently, the probability of every finite subset of $traces(I)$ is included in the system representation, and if $traces(I)$ is finite then $\mathcal{F}_I = \mathbb{P}(traces(I))$.

In order to check whether a system complies with a pSTAIRS specification we represent the system as a set of p-obligations. To ensure that all information from the cone-$\sigma$-field is contained in the representation we generate one p-obligation from every trace set in $\mathcal{F}_I$. The pSTAIRS representation $\langle I \rangle_d^p$ of the system $I$ is defined by:

$$\langle I \rangle_d^p \overset{\mathsf{def}}{=} \{((s, \mathcal{H}^{ll(d)} \setminus s), \{f_I(s)\}) \mid s \in \mathcal{F}_I \wedge s \neq \emptyset\} \tag{30}$$

The superscript $p$ means that $\langle I \rangle_d^p$ is a probabilistic representation, and is sometimes omitted when this is obvious from the context. The subscript $d$ means that the representation is related to the specification $d$, i.e. that only traces that occur exclusively on lifelines in $d$ are included as negative.

### 5.2 Compliance relations for single p-obligations

As for refinement, we first define compliance relations for single p-obligations since compliance with probabilistic specifications is defined in terms of compliance for single p-obligations:

$$(o, Q) \mapsto_{px} (o', Q') \overset{\mathsf{def}}{=} o \mapsto_x o' \wedge Q' \subseteq Q \tag{31}$$

where $x \in \{r, rr, nr\}$. The compliance relations for interaction obligations are defined by:

$$(p, n) \mapsto_r (p', n') \overset{\mathsf{def}}{=} n \subseteq n' \wedge p \subseteq p' \cup n' \tag{32}$$

$$(p, n) \mapsto_{rr} (p', n') \overset{\mathsf{def}}{=} (p, n) \mapsto_r (p', n') \wedge p \cap p' \neq \emptyset \tag{33}$$

$$(p, n) \mapsto_{nr} (p', n') \overset{\mathsf{def}}{=} (p, n) \mapsto_{rr} (p', n') \tag{34}$$

The compliance relations $\mapsto_{rr}$ and $\mapsto_{nr}$ allow inconclusive traces to be produced by the system, even if the corresponding refinement relations $\rightsquigarrow_{rr}$ and $\rightsquigarrow_{nr}$ do not allow inconclusive traces at the abstract level to become positive at the concrete level. The reason why the compliance relations allow inconclusive traces to be produced is the potential for implied scenarios (see “Restricted compliance relation” in Section 4.2 of [RRS07]). Implied scenarios must be taken into account when defining compliance relations since the system representations are complete while sequence diagram specifications may be partial.

The reason why $\mapsto_{nr}$ has been defined as a separate relation even though it is identical to $\mapsto_{rr}$ is to get matching subscripts on refinement and compliance and relations that belong together.

### 5.3 General, restricted general and narrowing general compliance

Similar to general refinement, a system $I$ is a (restricted) general compliance of a sequence diagram $d$ if every p-obligation in $[\![\ d\ ]\!]$ where 0 is not an acceptable probability is implemented by at least one p-obligation in $\langle I\rangle_d^p$:

$$[\![\ d\ ]\!] \mapsto_x \langle I\rangle_d^p \overset{\mathsf{def}}{=} \forall po \in [\![\ d\ ]\!] : 0 \notin \pi_2.po \Rightarrow \exists po' \in \langle I\rangle_d^p : po \mapsto_y po' \tag{35}$$

where $(x, y) \in \{(pg, pr), (prg, prr), (png, pnr)\}$. Note that the relations $\mapsto_{prg}$ and $\mapsto_{png}$ are identical since the relations $\mapsto_{prr}$ and $\mapsto_{pnr}$ are identical.

### 5.4 Limited, restricted limited and narrowing limited compliance

Similar to limited refinement, we now also require that every p-obligation obtained by Definition (30) is a member of a set whose combined sum is in compliance of at least one p-obligation in $[\![\ d\ ]\!]$:

$$\begin{aligned}
&[\![\ d\ ]\!] \mapsto_x \langle I\rangle_d^p \overset{\mathsf{def}}{=} \\
&\quad [\![\ d\ ]\!] \mapsto_y \langle I\rangle_d^p \wedge \\
&\quad \forall po' \in \langle I\rangle_d^p : \exists S \subseteq \langle I\rangle_d^p : \exists po \in [\![\ d\ ]\!] : po' \in S \wedge po \mapsto_z \bar{\bigoplus} S
\end{aligned} \tag{36}$$

where $(x, y, z) \in \{(pl, pg, pr), (prl, prg, prr), (pnl, png, pnr)\}$. Again note that the relations $\mapsto_{prl}$ and $\mapsto_{pnl}$ are identical.

### 5.5 Example

The specification S3 in Figure 9 is a probabilistic version of the gambling machine specified in the diagram S2 in [RRS07]. S3 requires that the probability of losing is exactly 0.9 and that the probability of winning is 0.1. Its semantics is given by

$$[\![\ \text{S3}\ ]\!] = \{(o_1, \{0.1\}), (o_2, \{0.9\}), (o_3, \{1\})\}$$

The interaction obligations $o_1$, $o_2$ and $o_3$ are given by

$$\begin{aligned}
&o_1 = \\
&\quad (\ \{\ \langle !di, ?di, !m(yw), ?m(yw), !do, ?do\rangle\ , \langle !qu, ?qu, !m(yw), ?m(yw), !do, ?do\rangle\ , \\
&\qquad \langle !di, ?di, !m(yw), !do, ?m(yw), ?do\rangle\ , \langle !qu, ?qu, !m(yw), !do, ?m(yw), ?do\rangle\ \}, \\
&\quad\ \ \{\ \langle !di, ?di, !m(yl), ?m(yl)\rangle\ , \langle !qu, ?qu, !m(yl), ?m(yl)\rangle\ , \\
&\qquad \langle !di, ?di, !m(yl), ?m(yl), !do, ?do\rangle\ , \langle !qu, ?qu, !m(yl), ?m(yl), !do, ?do\rangle\ , \\
&\qquad \langle !di, ?di, !m(yl), !do, ?m(yl), ?do\rangle\ , \langle !qu, ?qu, !m(yl), !do, ?m(yl), ?do\rangle\ \}\ )
\end{aligned}$$

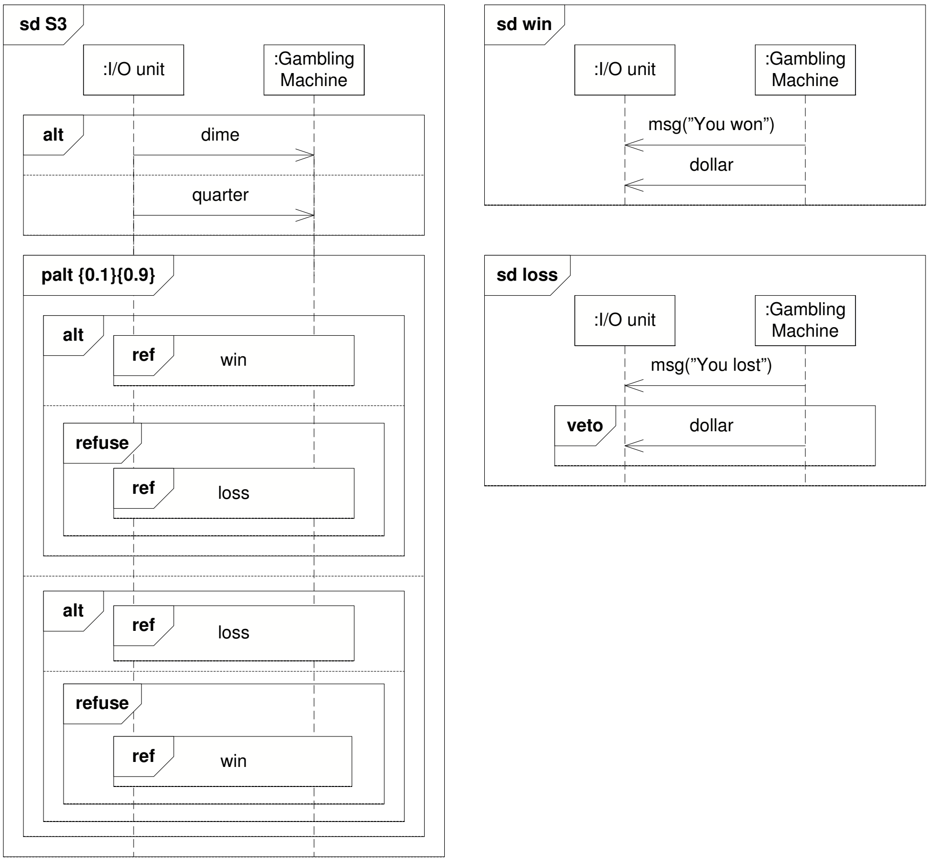

**Fig. 9.** A probabilistic gambling machine

$$
\begin{array}{l}
o_2 = \\
\quad (\ \{\ \langle !di, ?di, !m(yl), ?m(yl)\rangle\ , \langle !qu, ?qu, !m(yl), ?m(yl)\rangle\ \}, \\
\qquad \{\ \langle !di, ?di, !m(yw), ?m(yw), !do, ?do\rangle\ , \langle !qu, ?qu, !m(yw), ?m(yw), !do, ?do\rangle\ , \\
\qquad\quad \langle !di, ?di, !m(yw), !do, ?m(yw), ?do\rangle\ , \langle !qu, ?qu, !m(yw), !do, ?m(yw), ?do\rangle\ , \\
\qquad\quad \langle !di, ?di, !m(yl), ?m(yl), !do, ?do\rangle\ , \langle !qu, ?qu, !m(yl), ?m(yl), !do, ?do\rangle\ , \\
\qquad\quad \langle !di, ?di, !m(yl), !do, ?m(yl), ?do\rangle\ , \langle !qu, ?qu, !m(yl), !do, ?m(yl), ?do\rangle\ \}\ )
\end{array}
$$

$$
\begin{array}{l}
o_3 = \oplus\{o_1, o_2\} = \\
\quad (\ \{\ \langle !di, ?di, !m(yw), ?m(yw), !do, ?do\rangle\ , \langle !qu, ?qu, !m(yw), ?m(yw), !do, ?do\rangle\ , \\
\qquad\quad \langle !di, ?di, !m(yw), !do, ?m(yw), ?do\rangle\ , \langle !qu, ?qu, !m(yw), !do, ?m(yw), ?do\rangle\ , \\
\qquad\quad \langle !di, ?di, !m(yl), ?m(yl)\rangle\ , \langle !qu, ?qu, !m(yl), ?m(yl)\rangle\ \}, \\
\qquad \{\ \langle !di, ?di, !m(yl), ?m(yl), !do, ?do\rangle\ , \langle !qu, ?qu, !m(yl), ?m(yl), !do, ?do\rangle\ , \\
\qquad\quad \langle !di, ?di, !m(yl), !do, ?m(yl), ?do\rangle\ , \langle !qu, ?qu, !m(yl), !do, ?m(yl), ?do\rangle\ \}\ )
\end{array}
$$

Let $I$ be a system represented by the probability space $(traces(I), \mathcal{F}_I, f_I)$ where $\mathcal{F}_I$ is the cone-$\sigma$-field on $traces(I)$ and

$$
\begin{aligned}
traces(I) &= \{t_1, t_2, t_3\} \\
t_1 &= \langle !di, ?di, !m(yw), ?m(yw), !do, ?do\rangle \\
t_2 &= \langle !di, ?di, !m(yw), !do, ?m(yw), ?do\rangle \\
t_3 &= \langle !di, ?di, !m(yl), ?m(yl)\rangle \\
f_I(\{t_1\}) &= f_I(\{t_2\}) = 0.05 \\
f_I(\{t_3\}) &= 0.9
\end{aligned}
$$

Since $traces(I)$ is finite, every subset of $traces(I)$ is a member of $\mathcal{F}_I$, and we get $f_I(\{t_1, t_2\}) = 0.1$ and $f_I(\{t_1, t_2, t_3\}) = 1$. Every member of $\mathcal{F}_I$ gives rise to a p-obligation in $\langle I\rangle_d^p$. In particular, we have that

$$
\begin{aligned}
((\{t_3\}, \mathcal{H}^{ll(S3)} \setminus \{t_3\}), \{0.9\}) &\in \langle I\rangle_d^p \\
((\{t_1, t_2\}, \mathcal{H}^{ll(S3)} \setminus \{t_1, t_2\}), \{0.1\}) &\in \langle I\rangle_d^p \\
((\{t_1, t_2, t_3\}, \mathcal{H}^{ll(S3)} \setminus \{t_1, t_2, t_3\}), \{1\}) &\in \langle I\rangle_d^p
\end{aligned}
$$

The first of these three p-obligations complies with $(o_2, \{0.9\})$, the second complies with $(o_1, \{0.1\})$ and the third with $(o_3, \{1\})$ according to all of the compliance relations $\mapsto_{pr}$, $\mapsto_{prr}$ and $\mapsto_{pnr}$ defined for single p-obligations. We therefore get

$$
\begin{aligned}
\llbracket\ \text{S3}\ \rrbracket &\mapsto_{pg} \langle I\rangle_{S3}^p \\
\llbracket\ \text{S3}\ \rrbracket &\mapsto_{prg} \langle I\rangle_{S3}^p \\
\llbracket\ \text{S3}\ \rrbracket &\mapsto_{png} \langle I\rangle_{S3}^p
\end{aligned}
$$

We also have

$$
\begin{aligned}
\llbracket\ \text{S3}\ \rrbracket &\mapsto_{pl} \langle I\rangle_{S3}^p \\
\llbracket\ \text{S3}\ \rrbracket &\mapsto_{prl} \langle I\rangle_{S3}^p \\
\llbracket\ \text{S3}\ \rrbracket &\mapsto_{pnl} \langle I\rangle_{S3}^p
\end{aligned}
$$

To see this, observe that $\bar{\oplus}\langle I\rangle^p_{S3} = ((\{t_1, t_2, t_3\}, \mathcal{H}^{ll(S3)} \setminus \{t_1, t_2, t_3\}), \{1\})$. Since this p-obligation complies with a p-obligation in $[\![\ \mathrm{S3}\ ]\!]$, the condition that any p-obligation in $\langle I\rangle^p_{S3}$ is a member of a subset $S$ of $\langle I\rangle^p_{S3}$ such that $\bar{\oplus}S$ complies with a p-obligation in $[\![\ \mathrm{S3}\ ]\!]$ is easily fulfilled by choosing $S = \langle I\rangle^p_{S3}$.

### 5.6 Transitivity between refinement and compliance

Transitivity between refinement and compliance means that if $d$ is refined by $d'$ and system $I$ complies with $d'$, then $I$ complies also with $d$. Formally:

$$[\![\ d\ ]\!] \rightsquigarrow_x [\![\ d'\ ]\!] \wedge [\![\ d'\ ]\!] \mapsto_x \langle I\rangle^p_{d'} \Rightarrow [\![\ d\ ]\!] \mapsto_x \langle I\rangle^p_d \tag{37}$$

Transitivity between refinement and compliance is important as it ensures that a system complies with a specification if it complies with a refinement of the specification.

The following table summarizes results with respect to transitivity between refinement and compliance for different refinement and compliance relations. As $\rightsquigarrow_{prl}$ is not transitive it is not relevant here.

| $\rightsquigarrow_{pg}$ | $\rightsquigarrow_{prg}$ | $\rightsquigarrow_{pl}$ | $\rightsquigarrow_{png}$ | $\rightsquigarrow_{pnl}$ |
|---|---|---|---|---|
| Y: T16 | Y: T17 | Y: T18 | Y: T19 | Y: T20 |

## 6 The relation between inherent nondeterminism and probabilistic choice

Intuitively it seems clear that inherent nondeterminism (expressed by xalt in STAIRS) is closely related to probabilistic choice (expressed by palt in pSTAIRS). From a methodological perspective, it might be natural to use STAIRS in the early stage of a development process. At this stage the essential question is: what alternatives need to be possible? Later in the process we may want to specify with what probability the different alternatives should occur. This can be achieved by replacing all xalt operators with palt. Switching from pSTAIRS to STAIRS (by replacing palt operators with xalt) in a development process would not make much sense, since this would mean that all information regarding probabilities would be lost. In essence, this means that we want to ensure that compliance and refinement relations are preserved when switching from STAIRS to pSTAIRS (but not the other way around).

To facilitate a development process where xalt may be replaced with palt at some point we first provide a translation function from specifications with inherent nondeterminism to specifications with probabilistic choice. Then we show how the result of a translation corresponds to the original specification with respect to refinement and compliance.

### 6.1 Probabilistic interpretation of inherent nondeterminism

The xalt expresses a choice between alternatives that must all be represented both in further refinements of the specification and in a system that complies with the specification. Apart from this, nothing is said about the probabilities of each alternative. The palt expresses a probabilistic choice between alternatives. Unless 0 is an acceptable probability for an alternative, the alternative must be represented both in further refinements of the specification and in a system that complies with the specification. Therefore there should be some way of interpreting xalt in terms of palt. There are at least two approaches for doing this:

- Interpret an xalt operator as a set of palt operators, where each operand is assigned exactly one probability so that the sum of probabilities is 1. This means that a specification of the form $d_1$ xalt $d_2$ is interpreted as a set of specifications of the form $d_1;\{q_1\}$ palt $d_2;\{q_1\}$, where $q_1, q_2 > 0$ and $q_1 + q_2 = 1$. Recall that if $q_1 + q_2 \neq 1$ then we obtain a p-obligation with an empty probability set due to definition (9b), which means that the specification can not be complied with.
- Interpret an xalt operator as a single palt operator, where each operand may be assigned a set of probabilities. This means that a specification of the form $d_1$ xalt $d_2$ is interpreted as a specification of the form $d_1;Q_1$ palt $d_2;Q_2$ for some suitable probability sets $Q_1$ and $Q_2$.

With the first approach the underspecification with respect to probabilities implied by the xalt is reflected by the fact that a specification with xalt is translated to a *set* of specifications with palt instead of a single specification. This means that developers will have to maintain a set of specifications instead of a single specification if they want to retain some underspecification with respect to probabilities after switching from STAIRS to pSTAIRS. To avoid this we choose the second approach, in which a single specification with xalt corresponds to a single specification with palt. This also keeps things simple when we later explore the correspondence between specifications with xalt and specifications with palt.

The next question is what probability sets should be assigned to the operands when replacing an xalt operator with a palt operator. Since the only requirement of xalt is that all alternatives are represented both in further refinements and in the final system, the following probability sets are the natural candidates to evaluate: $[0, 1]$, $\langle 0, 1\rangle$ and $\langle 0, 1]$.

When deciding on which of these to choose we have to consider the different expressiveness of STAIRS and pSTAIRS. In STAIRS there is no way to distinguish between alternatives that need to occur with a probability higher than 0 and alternatives that that simply need to be possible; the only thing we know is that each alternative of an xalt operator needs to be possible. That an alternative can be possible even though its probability is 0 is illustrated by the process where a coin is tossed infinitely many times: the probability is 0 for each trace of this process.[6]

In pSTAIRS the refinement and compliance relations allow p-obligations with 0 as an acceptable probability to be ignored at the concrete level[7]. This design choice was made in order to allow specification of cases where an undesirable alternative is acceptable as long as its probability is not too high, but where it is also perfectly acceptable if the undesirable alternative does not occur at all. This allows us to capture and reason about soft real-time constraints [RHS05]. STAIRS cannot distinguish such alternatives, and requires all interaction obligations to be represented in a refinement and in the specified system. Therefore 0 cannot be a member of the probability sets we assign to the operands when replacing $\mathsf{xalt}$ with $\mathsf{palt}$. Otherwise the requirement that every operand should be represented in further refinement steps and the final system would be lost when replacing $\mathsf{xalt}$ with $\mathsf{palt}$. This means that the set $[0, 1]$ is out of the question.

The next candidate we look at is $\langle 0, 1\rangle$. Intuitively, this seems to be a good choice. By excluding 0 as an acceptable probability we ensure that each operand of the original $\mathsf{xalt}$ is represented in refinements and the specified system. And if 0 is not an acceptable probability for any operand then it seems natural that 1 should not be an acceptable probability for any operand. But this actually only applies in cases where the operands are mutually exclusive. Consider the specification $d = e \;\mathsf{xalt}\; e$ where $e$ is a single event. There is nothing wrong with this specification, even if the use of $\mathsf{xalt}$ in this case is unnecessary and the specification is of little practical relevance. It is clear that any system $I$ such that $traces(I) = \{\langle e\rangle\}$ complies with the specification. But consider now the specification $d' = \mathsf{palt}(e;\langle 0, 1\rangle, e;\langle 0, 1\rangle)$. This specification requires that $\langle I\rangle^{p}_{d'}$ contains a p-obligation whose probability set is a subset of $\langle 0, 1\rangle$. But if $traces(I) = \{\langle e\rangle\}$ then $f_I(\{\langle e\rangle\}) = 1$, and there is no p-obligation in $\langle I\rangle^{p}_{d'}$ whose probability set is a subset of $\langle 0, 1\rangle$. So $I$ does not comply with $d'$, even if it complies with $d$. We therefore also reject $\langle 0, 1\rangle$.

Hence we are left with $\langle 0, 1]$. Luckily, using the set $\langle 0, 1]$ we ensure that

- each operand of the original $\mathsf{xalt}$ is represented in refinements and the specified system (by excluding 0 from the acceptable probabilities),
- there is a correspondence between STAIRS and pSTAIRS in cases like the example with $d$ and $d'$ above (by including 1 among the acceptable probabilities) and

[6] To specify an infinite coin toss in STAIRS/pSTARIS requires use of the $\mathsf{loop}$ operator. This operator is defined in [HHRS06] for STAIRS and [RHS07a] for pSTAIRS, but is outside the scope of this paper.

[7] This does not mean that a specification of an infinite coin toss is meaningless in pSTAIRS. For such a specification will require that the system is able to produce any finite prefix of all traces representing the infinite coin toss with the appropriate probability, due to combined p-obligations obtained from Definition (9b). For example, the probability of producing a trace starting with heads should be 0.5, the probability of producing a trace starting with two consecutive heads should be 0.25, and so on.

- the xalt represents a very large degree of underspecification with respect to probabilities.

Based on these considerations we define a translator function $g$ that translates a sequence diagram with underspecification and inherent nondeterminism to a sequence diagram with underspecification and probabilistic choice:

$$g(d) \overset{\mathsf{def}}{=} \begin{cases} d & \text{if } d \in \mathcal{E} \cup \{\mathsf{skip}\} \\ op\ g(d_1) & \text{if } d = op\ d_1 \text{ for} \\ & \quad op \in \{\mathsf{refuse}, \mathsf{veto}\} \\ g(d_1)\ op\ g(d_2) & \text{if } d = d_1\ op\ d_2 \text{ for} \\ & \quad op \in \{\mathsf{alt}, \mathsf{seq}, \mathsf{par}\} \\ \mathsf{palt}(g(d_1);\langle 0,1], \ldots, g(d_n);\langle 0,1]) & \text{if } d = \mathsf{xalt}(d_1, \ldots, d_n) \end{cases} \tag{38}$$

For use in proofs and formulation of results we let $\mathcal{D}^u$ denote the set of all sequence diagrams with underspecification, $\mathcal{D}^i$ denote the set of all sequence diagrams with underspecification and inherent nondeterminism, and $\mathcal{D}^p$ denote the set of all sequence diagrams with underspecification and probabilistic choice. In other words:

- $\mathcal{D}^u$ denotes the set of all sequence diagrams that contains only operators from the set $OP = \{\mathsf{refuse}, \mathsf{seq}, \mathsf{par}, \mathsf{alt}, \mathsf{skip}\}$,
- $\mathcal{D}^i$ denotes the set of all sequence diagrams that contains only operators from the set $OP \cup \{\mathsf{xalt}\}$, and
- $\mathcal{D}^p$ denotes the set of all sequence diagrams that contains only operators from the set $OP \cup \{\mathsf{palt}\}$.

Hence, $\mathcal{D}^i$ is the domain of the translator function $g$. We easily see that $g(d) \in \mathcal{D}^p$ for any $d \in \mathcal{D}^i$.

### 6.2 Correspondence

In this section we present results concerning correspondence with respect to refinement and compliance when switching from STAIRS to pSTAIRS. Based on the evaluation in Section 4 we restrict our attention to the winners, i.e. limited and limited narrowing refinement and compliance.

As refinement and compliance relations for STAIRS specifications based on $\rightsquigarrow_{nr}$ and $\mapsto_{nr}$ were not defined in [RRS07], we need to give these definitions before presenting the correspondence results. The definitions are obtained by replacing $\rightsquigarrow_r$ with $\rightsquigarrow_{nr}$ and $\mapsto_r$ with $\mapsto_{nr}$ in the obvious way:

$$[\![\ d\ ]\!]^i \rightsquigarrow_{ng} [\![\ d'\ ]\!]^i \overset{\mathsf{def}}{=} \forall o \in [\![\ d\ ]\!]^i : \exists o' \in [\![\ d'\ ]\!]^i : o \rightsquigarrow_{nr} o' \tag{39}$$

$$\begin{aligned} [\![\ d\ ]\!]^i \rightsquigarrow_{nl} [\![\ d'\ ]\!]^i \overset{\mathsf{def}}{=}\ & [\![\ d\ ]\!]^i \rightsquigarrow_{ng} [\![\ d'\ ]\!]^i \\ & \wedge \forall o' \in [\![\ d'\ ]\!]^i : \exists o \in [\![\ d\ ]\!]^i : o \rightsquigarrow_{nr} o' \end{aligned} \tag{40}$$

$$[\![\ d\ ]\!]^i \mapsto_{ng} \langle I \rangle_d^i \overset{\mathsf{def}}{=} \forall o \in [\![\ d\ ]\!]^i : \exists o' \in \langle I \rangle_d^i : o \mapsto_{nr} o' \tag{41}$$

$$\begin{aligned} [\![\ d\ ]\!]^i \mapsto_{nl} \langle I \rangle_d^i \overset{\mathsf{def}}{=}\ & [\![\ d\ ]\!]^i \mapsto_{ng} \langle I \rangle_d^i \\ & \wedge \forall o' \in \langle I \rangle_d^i : \exists o \in [\![\ d\ ]\!]^i : o \mapsto_{nr} o' \end{aligned} \tag{42}$$

We are now ready to give the relevant correspondence results. Theorem 1 states the correspondence with respect to limited compliance:

**Theorem 1 (Correspondence between $\mapsto_l$ and $\mapsto_{pl}$).** *Let $d \in \mathcal{D}^i$. Then*

$$(\forall (o, \{q\}) \in \langle I \rangle_d^p : q > 0) \wedge [\![\ d\ ]\!]^i \mapsto_l \langle I \rangle_d^i \Rightarrow [\![\ g(d)\ ]\!]^p \mapsto_{pl} \langle I \rangle_d^p$$

The left conjunct of the antecedent in Theorem 1 requires an explanation. Since the probability sets assigned to the operands of a palt when translating an xalt does not contain 0, it is possible to produce an example where a system is in limited compliance with a STAIRS specification, but not with its translation to pSTAIRS. This is done by ensuring that the system produces a trace with probability 0 so that the resulting p-obligation in the system representation does not represent any p-obligation in the specification. This is illustrated in Lemma 55 in Appendix C. Hence correspondence between $\mapsto_l$ and $\mapsto_{pl}$ holds only for systems where the probability for all p-obligations is greater than 0.

For the correspondence with respect to narrowing compliance another condition has to be added, which is due to the $\bar{\oplus}$ operator used when defining the semantics of palt. For any set $S$ of p-obligations, all traces that are inconclusive in at least one p-obligation in $S$ are inconclusive also in the p-obligation $\bar{\oplus} S$. Hence, the use of palt may generate p-obligations with more inconclusive traces than any of the original p-obligations in $S$. If these new p-obligations are not represented in a system then we may have compliance in the non-probabilistic case, but not in the probabilistic case. An example of such a case is given in Lemma 56 in Appendix C.

Since xalt is translated to palt when switching from the non-probabilistic to the probabilistic case, the above situation can be avoided by ensuring that the inconclusive traces are the same for every interaction obligation of every operand of an xalt. We use the predicate $E(d)$ to denote that the diagram $d$ fulfills this condition. Formally, $E(d)$ holds iff for every subdiagram of $d$ of the form xalt$(d_1, \ldots, d_m)$ there exists a set of traces $s$ such that

$$\forall (p, n) \in \bigcup_{i=1}^{m} [\![\ d_i\ ]\!] : p \cup n = s \tag{43}$$

Theorem 2 states the correspondence with respect to narrowing limited compliance when switching from STAIRS to pSTAIRS:

**Theorem 2 (Correspondence between $\mapsto_{nl}$ and $\mapsto_{pnl}$).** *Let $d \in \mathcal{D}^i$. Then*

$$E(d) \wedge (\forall (o, \{q\}) \in \langle I \rangle_d^p : q > 0) \wedge [\![\ d\ ]\!]^i \mapsto_{nl} \langle I \rangle_d^i \Rightarrow [\![\ g(d)\ ]\!]^p \mapsto_{pnl} \langle I \rangle_d^p$$

We now look at correspondence theorems with respect to refinement. For limited refinement we need to ensure that the specification at the concrete level is xalt-*normal* in order to achieve correspondence. A specification $d \in \mathcal{D}^i$ is xalt-normal, written $N(d)$, iff either it does not contain any xalt at all or it is of the form xalt$(d_1, \ldots, d_m)$, where none of the operands $d_j$ contains xalt. In other words, if $d$ contains an $\mathsf{xalt}$ then $\mathsf{xalt}$ may occur only at the outermost level. Formally:

$$N(d) \overset{\mathsf{def}}{=} d \in \mathcal{D}^u \vee (d = \mathsf{xalt}(d_1, \ldots, d_m) \wedge \forall j \leq m : d_j \in \mathcal{D}^u) \qquad (44)$$

The reason why we need this requirement is that $\mathsf{palt}$, unlike $\mathsf{xalt}$, is not distributive with respect to the composition operators in general. This is because $\bar{\oplus}$ is not distributive with respect to all operators at the semantic level; for example $\bar{\oplus}(S_1 \succsim S_2) = \bar{\oplus}S_1 \succsim \bar{\oplus}S_2$ does not hold for all sets of p-obligations $S_1$ and $S_2$. In the example given in Lemma 59 in Appendix C this is exploited to produce specifications where correspondence does not hold because the specification at the concrete level is not $\mathsf{xalt}$-normal.

Theorem 3 states the correspondence with respect to limited refinement when switching from STAIRS to pSTAIRS:

**Theorem 3 (Correspondence between $\rightsquigarrow_l$ and $\rightsquigarrow_{pl}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$N(d') \wedge E(d') \wedge [\![\ d\ ]\!]^i \rightsquigarrow_l [\![\ d'\ ]\!]^i \Rightarrow [\![\ g(d)\ ]\!]^p \rightsquigarrow_{pl} [\![\ g(d')\ ]\!]^p$$

In the case of narrowing limited refinement, we also need to require that the specification at the abstract level is $\mathsf{xalt}$-normal. The need for this requirement is illustrated by the example given in Lemma 62 in Appendix C.

Theorem 4 states the correspondence with respect to narrowing limited refinement when switching from STAIRS to pSTAIRS:

**Theorem 4 (Correspondence between $\rightsquigarrow_{nl}$ and $\rightsquigarrow_{pnl}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$N(d) \wedge N(d') \wedge E(d') \wedge [\![\ d\ ]\!]^i \rightsquigarrow_{nl} [\![\ d'\ ]\!]^i \Rightarrow [\![\ g(d)\ ]\!]^p \rightsquigarrow_{pnl} [\![\ g(d')\ ]\!]^p$$

One may ask whether the extra conditions of the form $E(d)$ and $N(d)$ that are included in the antecedents of the correspondence theorems have a significant negative impact on the usefulness of the theorems from a methodological point of view. Fortunately this is not the case, since these requirements can easily be fulfilled. The requirement $E(d)$ can be fulfilled by using $\mathsf{exxalt}$[8] for exclusive alternatives instead of $\mathsf{xalt}$ in $d$. As argued in Section 3.2, $\mathsf{exxalt}$ will normally be a suitable operator in all cases where an $\mathsf{xalt}$ could be used in a practical specification.

With respect to the requirements of the form $N(d)$, it is shown by Lemma 38 in Appendix C that any specification $d \in \mathcal{D}^i$ can be rewritten into an equivalent specification $d'$ that is $\mathsf{xalt}$-normal, i.e. that $[\![\ d\ ]\!]^i = [\![\ d'\ ]\!]^i$ and $N(d')$ holds. This rewrite, which could be automated, can therefore be performed before switching to pSTAIRS without affecting the refinement relations established in STAIRS.

[8] This operator is defined by Definition (56), Appendix A.

## 7 Related work

In [RRS07] we investigated the relationship between computer systems and sequence diagrams for sequence diagrams with underspecification and sequence diagrams with both inherent nondeterminism and underspecification. The basis of [RRS07] as well as this paper is sequence diagrams as defined in e.g. UML 2.1 [OMG06]. As the focus of this paper is on compliance relations and not sequence diagrams as such, we have covered only the most essential of the UML 2.1 operators. In addition, we have considered operators for specifying inherent nondeterminism and probabilistic choice. These operators are not found in UML 2.1, and neither in most other variants of sequence diagrams such as Message Sequence Charts (MSCs) [ITU99].

For related work on the relationship between computer systems and sequence diagrams without probabilistic choice we refer to [RRS07]. For probabilistic sequence diagrams, we are not aware of any paper about refinement or the relationship to computer systems. However, these issues has been investigated for other specification languages.

In [MM05] a probabilistic extension of Dijkstra's Guarded Command Language called pGCL is presented. The language allows nondeterministic (demonic/angelic) choice as well as probabilistic choice to be expressed, and pGCL is a specification language as well as a programming language. Hence there is no distinction between refinement and compliance. Refinement is defined in terms of sets of behaviours. Abstraction is inclusion and refinement is reverse inclusion.

In [JHSY94], refinement is defined for transition systems with nondeterministic choice and probabilistic choice. As in [MM05], nondeterministic choice is used to represent underspecification, and refinement corresponds to restricting the possible behaviour. In [JHSY94] a test is a probabilistic transition system with a defined set of success states; the probabilities of success is obtained by composing a test with the system to be tested. This kind of probabilistic tests have very strong distinguishing power, so that certain systems that are equivalent in non-probabilistic testing will no longer be equivalent in probabilistic testing. Therefore an alternative weaker notion of testing called reward testing is proposed. A reward test does not have probabilistic choice. Instead the end states are assigned a nonnegative *reward*, and the outcome of a test is given as expected rewards instead of probabilities of success.

Both pGCL [MM05] and the transition systems of [JHSY94] are complete specifications in the sense that there is no notion of inconclusive behavior as there is for sequence diagrams.

## 8 Conclusions

Building on [RRS07] we have defined different refinement relations and their corresponding compliance relations for sequence diagrams with probabilistic choice. Furthermore we have investigated these relations with mathematical properties that are desirable from a methodological point of view. For the relations that fulfill the desired properties we have established correspondence theorems between the non-probabilistic and the probabilistic case.

Our general compliance checking procedure for relating systems and sequence diagrams was given in Section 1. Together with the defined refinement and compliance relations, as well as the correspondence theorems, the procedure meets the requirements stated in Section 2 in the following sense:

1. The procedure is independent of any particular programming language or paradigm. All we require, is that there exists some means to obtain the probability space representing the system (with respect to an asynchronous communication paradigm).
2. The notion of compliance is a special case of refinement, as we use the refinement relations in the definitions of the compliance relations. Whatever refinement relation is used between two sequence diagrams, any implementation of the refinement is also an implementation of the original diagram.
3. The translator function $g$ defined in Section 6.1 shows how a sequence diagram with inherent nondeterminism can be translated to a sequence diagram with probabilistic choice. The correspondence theorems presented in Section 6.2 give the necessary conditions for ensuring that refinement and compliance relations are preserved when $g$ is used to switch from the non-probabilistic to the probabilistic case by the application of $g$. These conditions can easily be fulfilled for practical specifications. Together, the translator function $g$ and the correspondence theorems therefore facilitates a development method where probabilistic information can be left out during the early stages of development.
4. The approach is faithful to the UML 2.1 standard, both with respect to the underlying semantic model using sets of positive and negative traces, and with respect to the semantics given for each concrete operator. In particular, all of our definitions take into account the partial nature of sequence diagrams.

In this paper we have only considered sequence diagrams without external input and output. Our results may be generalized to handle also sequence diagrams with such external communication by in each case defining an adversary representing the environment of the system, and then checking compliance under the assumption of this adversary.

The research on which this paper reports has been carried out within the context of the IKT-2010 project SARDAS (15295/431) and the IKT SOS project ENFORCE (164382/V30), both funded by the Research Council of Norway. We thank Thomas Weigert, Øystein Haugen, Rolv Bræk, Birger Møller-Pedersen, Mass Soldal Lund and Judith Rossebø for useful discussions related to this work.

## References

[Bré94] Pierre Brémaud. *An Introduction to Probabilistic Modeling*. Springer, 1994.

[Dud02] Richard M. Dudley. *Real Analysis and Probability.* Cambridge studies in advanced mathematics. Cambridge, 2002.

[HHRS05] Øystein Haugen, Knut Eilif Husa, Ragnhild Kobro Runde, and Ketil Stølen. STAIRS towards formal design with sequence diagrams. *Journal of Software and Systems Modeling*, 22(4):349–458, 2005.

[HHRS06] Øystein Haugen, Knut Eilif Husa, Ragnhild Kobro Runde, and Ketil Stølen. Why timed sequence diagrams require three-event semantics. Technical Report 309, Department of Informatics, University of Oslo, 2006.

[ITU99] International Telecommunication Union. *Recommendation Z.120 — Message Sequence Chart (MSC)*, 1999.

[JHSY94] Bengt Jonsson, Chris Ho-Stuart, and Wang Yi. Testing and Refinement for Nondeterministic and Probabilistic Processes. In H. Langmaack, W.-P. de Roever, and J. Vytopil, editors, *Formal Techniques in Real-Time and Fault-Tolerant Systems*, volume 863, pages 418–430. Springer, 1994.

[MM05] Annabelle McIver and Carroll Morgan. *Abstraction, Refinement and Proof for Probabilistic Systems.* Springer, 2005.

[OMG06] Object Management Group. *UML 2.1 Superstructure Specification*, document: ptc/06-04-02 edition, 2006.

[RHS05] Atle Refsdal, Knut Eilif Husa, and Ketil Stølen. Specification and refinement of soft real-time requirements using sequence diagrams. In *Proc. Formal Modeling and Analysis of Timed Systems: Third International Conference, FORMATS, 2005*, number 3829 in Lecture Notes in Computer Science, pages 32–48. Springer, 2005.

[RHS07a] Atle Refsdal, Knut Eilif Husa, and Ketil Stølen. Specification and refinement of soft real-time requirements using sequence diagrams. Technical Report 323, Department of Informatics, University of Oslo, 2007.

[RHS07b] Ragnhild Kobro Runde, Øystein Haugen, and Ketil Stølen. Refining UML interactions with underspecification and nondeterminism. Technical Report 325, Department of Informatics, University of Oslo, 2007.

[RRS07] Ragnhild Kobro Runde, Atle Refsdal, and Ketil Stølen. Relating computer systems to sequence diagrams with underspecification, inherent nondeterminism and probabilistic choice, Part 1. Technical Report 346, Department of Informatics, University of Oslo, 2007.

[Seg95] Roberto Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems.* PhD thesis, Massachusetts Institute of Technology, 1995.

[Sko05] A. V. Skorokhod. *Basic Principles and Applications of Probability Theory.* Springer, 2005.

# A Additional definitions

In the main section of this report we combined some definitions in order to save space. For better reference in proofs we now give individual definitions. Let $O_1$ and $O_2$ be sets of p-obligations. Then

$$
\begin{aligned}
O_1 \parallel O_2 &\overset{\mathsf{def}}{=} \{((o_1 \parallel o_2), Q_1 * Q_2) \mid (o_1, Q_1) \in O_1 \wedge (o_2, Q_2) \in O_2\} && (45)\\
O_1 \succsim O_2 &\overset{\mathsf{def}}{=} \{((o_1 \succsim o_2), Q_1 * Q_2) \mid (o_1, Q_1) \in O_1 \wedge (o_2, Q_2) \in O_2\} && (46)\\
O_1 \uplus O_2 &\overset{\mathsf{def}}{=} \{((o_1 \uplus o_2), Q_1 * Q_2) \mid (o_1, Q_1) \in O_1 \wedge (o_2, Q_2) \in O_2\} && (47)\\
\dagger O_1 &\overset{\mathsf{def}}{=} \{(\dagger o_1, Q_1) \mid (o_1, Q_1) \in O_1\} && (48)
\end{aligned}
$$

Operations for parallel composition, weak sequencing, inner union and negation for p-obligations were not explicitly defined in the main section. They are defined by

$$
\begin{aligned}
(o_1, Q_1) \parallel (o_2, Q_2) &\overset{\mathsf{def}}{=} (o_1 \parallel o_2, Q_1 * Q_2) && (49)\\
(o_1, Q_1) \succsim (o_2, Q_2) &\overset{\mathsf{def}}{=} (o_1 \succsim o_2, Q_1 * Q_2) && (50)\\
(o_1, Q_1) \uplus (o_2, Q_2) &\overset{\mathsf{def}}{=} (o_1 \uplus o_2, Q_1 * Q_2) && (51)\\
\dagger(o_1, Q_1) &\overset{\mathsf{def}}{=} (\dagger o_1, Q_1) && (52)
\end{aligned}
$$

We also define multiplication of a p-obligation or a set of p-obligations with a probability set:

$$
\begin{aligned}
(o, Q) * Q' &\overset{\mathsf{def}}{=} (o, Q * Q') && (53)\\
O * Q' &\overset{\mathsf{def}}{=} \{(o, Q * Q') \mid (o, Q) \in O\} && (54)
\end{aligned}
$$

When exploring the relationship between STAIRS and pSTAIRS it is convenient to have an n-ary $\mathsf{xalt}$ operator, where $n \geq 2$. This is defined by

$$
[\![\ \mathsf{xalt}(d_1, \ldots, d_n)\ ]\!]^i = \bigcup_{j=1}^{m} [\![\ d_j\ ]\!]^i \qquad (55)
$$

We easily verify that any specification with n-ary $\mathsf{xalt}$ operators can be rewritten into an equivalent specification with only binary $\mathsf{xalt}$ operators.

Corresponding to $\mathsf{expalt}$ for probabilistic specifications we define the operator $\mathsf{exxalt}$ for specifications with inherent nondeterminism.

$$
\begin{aligned}
&[\![\ \mathsf{exxalt}(d_1, \ldots, d_n)\ ]\!] \overset{\mathsf{def}}{=} && (56)\\
&\quad [\![\ \mathsf{xalt}((d_1 \ \mathsf{alt}\ \mathsf{refuse}(d_2 \ \mathsf{alt}\ \ldots\ \mathsf{alt}\ d_n)),\\
&\qquad\qquad \ldots\\
&\qquad\qquad (d_n \ \mathsf{alt}\ \mathsf{refuse}(d_1 \ \mathsf{alt}\ \ldots\ \mathsf{alt}\ d_{n-1})))\ ]\!]
\end{aligned}
$$

## B Shorthand notation

To save space in the proofs we will sometimes use $o$, $o_i$ and $o'$ as shorthand notation for $(p, n)$, $(p_i, n_i)$ and $(p', n')$, respectively. We also use $po$, $po_i$ and $po'$ as shorthand notation for $(o, Q)$, $(o_i, Q_i)$ and $(o', Q')$, respectively. This means that as a notational convention we have

$$\begin{aligned} po &= (o, Q) = ((p, n), Q) \\ po_i &= (o_i, Q_i) = ((p_i, n_i), Q_i) \\ po' &= (o', Q') = ((p', n'), Q') \end{aligned}$$

For simpler notation we also introduce the function $trs$ that returns the positive and negative traces of a p-obligation. Formally:

$$trs(((p, n), Q)) \stackrel{\mathsf{def}}{=} p \cup n \tag{57}$$

for any p-obligation $((p, n), Q)$.

For the example specifications given in proofs we write $ab$ as shorthand for $!a$ $\mathsf{seq}$ $?a$ $\mathsf{seq}$ $!b$ $\mathsf{seq}$ $?b$, and assume that the specification contains only one lifeline, which is both transmitter and receiver for all messages. Similarly, we write $\langle ab \rangle$ as shorthand for $\langle !a, ?a, !b, ?b \rangle$.

# C Proofs

In this section we state and prove each individual theorem. Theorems that are proved in other technical reports are not included. The following tables give the page number for each theorem and lemma. A reference is also given to results whose proof uses the relevant lemma or theorem. Some lemmas that are not used in any other proofs are included because they illustrate why alternative (and usually stronger) versions of certain theorems do not hold.

| Result | Page | Used in the proof of |
|---|---:|---|
| Lemma 1 | 43 | L13, L17, L19, T12, T32 |
| Lemma 2 | 44 | L7, L11, L18, L21, L42, T12, T15, T18, T20 |
| Lemma 3 | 45 | L11, T29, T30, T31, T44, T45, T46 |
| Lemma 4 | 46 | L11, L22, T29, T44 |
| Lemma 5 | 51 | L11, L23 T30, T45 |
| Lemma 6 | 51 | L11, T31, T46 |
| Lemma 7 | 52 | L11 |
| Lemma 8 | 53 | L11, T28, L54, T43 |
| Lemma 9 | 54 | L11, L45, T28, L54 |
| Lemma 10 | 54 | L11, L20, T32 |
| Lemma 11 | 55 | L12, T12, T18, T29, T30, T31, T32 |
| Lemma 12 | 58 | L13, L22, L23, L24, T15, T20, T44, T45, T46, T47 |
| Lemma 13 | 58 | T15, T20, T47 |
| Lemma 14 | 60 | T43 |
| Lemma 15 | 60 | T17 |
| Lemma 16 | 60 | L17 |
| Lemma 17 | 63 | T18 |
| Lemma 18 | 64 | T29, T30, T31, T44, T45, T46, |
| Lemma 19 | 65 | L24, T31, T46 |
| Lemma 20 | 67 | T47 |
| Lemma 21 | 67 | T32, T47 |
| Lemma 22 | 68 | T44 |
| Lemma 23 | 71 | T45 |
| Lemma 24 | 71 | T46 |
| Lemma 25 | 72 | T44, T45, T46 |
| Lemma 26 | 73 | T44, T45, T46 |
| Lemma 27 | 73 | L28 |
| Lemma 28 | 76 | T1, T2 |
| Lemma 29 | 76 | L30, L33 |
| Lemma 30 | 77 | L35 |
| Lemma 31 | 78 | L32, L36 |

| Result | Page | Used in the proof of |
|---|---|---|
| Lemma 32 | 79 | L33, T1, T2, T3, T4 |
| Lemma 33 | 82 | T1, T2, T3, T4 |
| Lemma 34 | 84 | L39, L43, L44, T1, T2, T3, T4 |
| Lemma 35 | 86 | L44, T1, T3, T4 |
| Lemma 36 | 88 | T1, T2, T3, T4 |
| Lemma 37 | 90 | L38 |
| Lemma 38 | 91 | - |
| Lemma 39 | 91 | T3, T4 |
| Lemma 40 | 95 | T29, T44 |
| Lemma 41 | 97 | T30, T45 |
| Lemma 42 | 98 | T29, T30, T31, T44, T45, T46 |
| Lemma 43 | 99 | L44, T4 |
| Lemma 44 | 102 | T2 |
| Lemma 45 | 116 | T21 |
| Lemma 46 | 118 | T23, L54 |
| Lemma 47 | 119 | T38 |
| Lemma 48 | 119 | T24 |
| Lemma 49 | 120 | T39 |
| Lemma 50 | 120 | T40 |
| Lemma 51 | 121 | T41 |
| Lemma 52 | 121 | T25 |
| Lemma 53 | 122 | T26 |
| Lemma 54 | 127 | T33 |
| Lemma 55 | 139 | - |
| Lemma 56 | 144 | - |
| Lemma 57 | 144 | - |
| Lemma 58 | 154 | - |
| Lemma 59 | 154 | - |
| Lemma 60 | 155 | - |
| Lemma 61 | 156 | - |
| Lemma 62 | 156 | - |

| Result | Page | Used in the proof of |
|---|---|---|
| Theorem 1 | 135 | - |
| Theorem 2 | 139 | - |
| Theorem 3 | 145 | - |
| Theorem 4 | 148 | - |
| Theorem 5 | 41 | T4, T14, T15, T47 |
| Theorem 6 | 41 | T2, T20 |
| Theorem 7 | 41 | L14, L47 |
| Theorem 8 | 42 | L49 |
| Theorem 9 | 42 | L50 |

| Result | Page | Used in the proof of |
|---|---|---|
| Theorem 10 | 42 | L51 |
| Theorem 11 | 102 | - |
| Theorem 12 | 103 | - |
| Theorem 13 | 105 | - |
| Theorem 14 | 106 | T15 |
| Theorem 15 | 106 | - |
| Theorem 16 | 108 | T18 |
| Theorem 17 | 109 | T19 |
| Theorem 18 | 109 | - |
| Theorem 19 | 110 | T20 |
| Theorem 20 | 110 | - |
| Theorem 21 | 117 | T28 |
| Theorem 22 | 117 | - |
| Theorem 23 | 119 | - |
| Theorem 24 | 121 | - |
| Theorem 25 | 121 | - |
| Theorem 26 | 122 | - |
| Theorem 27 | 122 | - |
| Theorem 28 | 123 | - |
| Theorem 29 | 124 | - |
| Theorem 30 | 125 | - |
| Theorem 31 | 125 | - |
| Theorem 32 | 126 | - |
| Theorem 33 | 128 | - |
| Theorem 34 | 128 | - |
| Theorem 35 | 129 | - |
| Theorem 36 | 129 | - |
| Theorem 37 | 129 | - |
| Theorem 38 | 130 | T43 |
| Theorem 39 | 130 | T44, T45, T46 |
| Theorem 40 | 130 | - |
| Theorem 41 | 130 | - |
| Theorem 42 | 130 | - |
| Theorem 43 | 130 | - |
| Theorem 44 | 131 | - |
| Theorem 45 | 132 | - |
| Theorem 46 | 133 | - |
| Theorem 47 | 133 | - |

### C.1 Specifications without probabilistic choice related to $\rightsquigarrow_{nr}$.

This section includes proofs for specification without probabilistic choice related to the refinement relation $\rightsquigarrow_{nr}$. These proofs are included in this report (Part 2) since the refinement relation $\rightsquigarrow_{nr}$ was not included in [RRS07].

**Theorem 5 (Transitivity of $\rightsquigarrow_{nr}$).** *Let $d$, $d'$ and $d''$ be sequence diagrams in $\mathcal{D}^u$. Then*

$$[\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d'\ ]\!]^u \wedge [\![\ d'\ ]\!]^u \rightsquigarrow_{nr} [\![\ d''\ ]\!]^u \Rightarrow [\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d''\ ]\!]^u$$

PROOF.

⟨1⟩1. ASSUME: $[\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d'\ ]\!]^u \wedge [\![\ d'\ ]\!]^u \rightsquigarrow_{nr} [\![\ d''\ ]\!]^u$
PROVE: $[\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d''\ ]\!]^u$
⟨2⟩1. $[\![\ d\ ]\!]^u \rightsquigarrow_{r} [\![\ d''\ ]\!]^u$
PROOF: By assumption ⟨1⟩1 and Lemma 26 in [HHRS06]
⟨2⟩2. LET: $(p, n) = [\![\ d\ ]\!]^u$
$(p', n') = [\![\ d'\ ]\!]^u$
$(p'', n'') = [\![\ d''\ ]\!]^u$
⟨2⟩3. $p \cup n = p' \cup n' \wedge p' \cup n' = p'' \cup n''$
PROOF: By assumption ⟨1⟩1
⟨2⟩4. Q.E.D.
PROOF: By ⟨2⟩1 and ⟨2⟩3
⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

**Theorem 6 (Transitivity between refinement and compliance for $\rightsquigarrow_{nr}$).** *Let $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^u$. Then*

$$[\![\ d_1\ ]\!]^u \rightsquigarrow_{nr} [\![\ d_2\ ]\!]^u \wedge [\![\ d_2\ ]\!]^u \mapsto_{nr} \langle I \rangle^u_{d_2} \Rightarrow [\![\ d_1\ ]\!]^u \mapsto_{nr} \langle I \rangle^u_{d_1}$$

PROOF. This is a special case of Theorem 7 in [RRS07], since $[\![\ d_1\ ]\!]^u \rightsquigarrow_{nr} [\![\ d_2\ ]\!]^u$ implies $[\![\ d_1\ ]\!]^u \rightsquigarrow_{rr} [\![\ d_2\ ]\!]^u$, and the definitions of $\mapsto_{rr}$ and $\mapsto_{nr}$ are identical. □

**Theorem 7 (Monotonicity of refuse w.r.t $\rightsquigarrow_{nr}$).** *Let $d \in \mathcal{D}^u$. Then*

$$[\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d'\ ]\!]^u \Rightarrow [\![\ \mathsf{refuse}\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ \mathsf{refuse}\ d'\ ]\!]^u$$

PROOF.

⟨1⟩1. ASSUME: $[\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d'\ ]\!]^u$
PROVE: $[\![\ \mathsf{refuse}\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ \mathsf{refuse}\ d'\ ]\!]^u$
⟨2⟩1. $[\![\ \mathsf{refuse}\ d\ ]\!]^u \rightsquigarrow_{r} [\![\ \mathsf{refuse}\ d'\ ]\!]^u$
⟨3⟩1. $[\![\ d\ ]\!]^u \rightsquigarrow_{nr} [\![\ d'\ ]\!]^u$
PROOF: By assumption ⟨1⟩1
⟨3⟩2. Q.E.D.
PROOF: By ⟨3⟩1 and Lemma 4 in [RHS07b]
⟨2⟩2. $\pi_1.[\![\ \mathsf{refuse}\ d\ ]\!]^u \cup \pi_2.[\![\ \mathsf{refuse}\ d\ ]\!]^u = \pi_1.[\![\ \mathsf{refuse}\ d'\ ]\!]^u \cup \pi_2.[\![\ \mathsf{refuse}\ d'\ ]\!]^u$
⟨3⟩1. LET: $(p, n) = [\![\ d\ ]\!]^u$
$(p', n') = [\![\ d'\ ]\!]^u$
⟨3⟩2. $p \cup n = p' \cup n'$

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

$\langle 3\rangle 3.$ $\llbracket\ \mathsf{refuse}\ d\ \rrbracket^u = (\emptyset, p \cup n) \wedge \llbracket\ \mathsf{refuse}\ d'\ \rrbracket^u = (\emptyset, p' \cup n')$

PROOF: By definition (8) in [RRS07]

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

PROOF: By $\langle 3\rangle 2$ and $\langle 3\rangle 3$

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

PROOF: by $\langle 2\rangle 1$ and $\langle 2\rangle 2$

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

PROOF: $\Rightarrow$-rule

□

**Theorem 8 (Monotonicity of $\mathsf{seq}$ w.r.t $\rightsquigarrow_{nr}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^u$. Then*

$$\llbracket\ d_1\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \rrbracket^u \wedge \llbracket\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_2'\ \rrbracket^u \Rightarrow \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket^u$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $\llbracket\ d_1\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \rrbracket^u \wedge \llbracket\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_2'\ \rrbracket^u$

PROVE: $\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket^u$

$\langle 2\rangle 1.$ $\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket^u \rightsquigarrow_{r} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket^u$

PROOF: By assumption $\langle 1\rangle 1$ and Lemma 30 in [HHRS06]

$\langle 2\rangle 2.$ $\pi_1.(\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket^u) \cup \pi_2.(\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket^u) = \pi_1.(\llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket^u) \cup \pi_2.(\llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket^u)$

$\langle 3\rangle 1.$ LET: $(p_i, n_i) = \llbracket\ d_i\ \rrbracket$ and $(p_i', n_i') = \llbracket\ d_i'\ \rrbracket$ for $i \in \{1, 2\}$

$\langle 3\rangle 2.$ $p_1 \cup n_1 = p_1' \cup n_1' \wedge p_2 \cup n_2 = p_2' \cup n_2'$

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

$\langle 3\rangle 3.$ $(p_1 \succsim p_2) \cup (n_1 \succsim p_2) \cup (n_1 \succsim n_2) \cup (p_1 \succsim n_2) = (p_1' \succsim p_2') \cup (n_1' \succsim p_2') \cup (n_1' \succsim n_2') \cup (p_1' \succsim n_2')$

PROOF: By $\langle 3\rangle 2$

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

PROOF: By $\langle 3\rangle 3$ and definition (7) in [RRS07]

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

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

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

PROOF: $\Rightarrow$-rule

□

**Theorem 9 (Monotonicity of $\mathsf{par}$ w.r.t $\rightsquigarrow_{nr}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^u$. Then*

$$\llbracket\ d_1\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \rrbracket^u \wedge \llbracket\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_2'\ \rrbracket^u \Rightarrow \llbracket\ d_1\ \mathsf{par}\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \mathsf{par}\ d_2'\ \rrbracket^u$$

PROOF. The proof is similar to the proof for Theorem 8; just replace $\mathsf{seq}$ with $\mathsf{par}$, $\succsim$ with $\|$ and the reference to Lemma 30 in [HHRS06] with a reference to Lemma 31 in [HHRS06]. □

**Theorem 10 (Monotonicity of $\mathsf{alt}$ w.r.t $\rightsquigarrow_{nr}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^u$. Then*

$$\llbracket\ d_1\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \rrbracket^u \wedge \llbracket\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_2'\ \rrbracket^u \Rightarrow \llbracket\ d_1\ \mathsf{alt}\ d_2\ \rrbracket^u \rightsquigarrow_{nr} \llbracket\ d_1'\ \mathsf{alt}\ d_2'\ \rrbracket^u$$

PROOF.

⟨1⟩1. ASSUME: $[\![\ d_1\ ]\!]^u \rightsquigarrow_{nr} [\![\ d_1'\ ]\!]^u \wedge [\![\ d_2\ ]\!]^u \rightsquigarrow_{nr} [\![\ d_2'\ ]\!]^u$
PROVE: $[\![\ d_1 \ \mathsf{alt}\ d_2\ ]\!]^u \rightsquigarrow_{nr} [\![\ d_1' \ \mathsf{alt}\ d_2'\ ]\!]^u$

⟨2⟩1. $[\![\ d_1 \ \mathsf{alt}\ d_2\ ]\!]^u \rightsquigarrow_{r} [\![\ d_1' \ \mathsf{alt}\ d_2'\ ]\!]^u$
PROOF: By assumption ⟨1⟩1 and Theorem 11 in [RRS07]

⟨2⟩2. $\pi_1.([\![\ d_1 \ \mathsf{alt}\ d_2\ ]\!]^u) \cup \pi_2.([\![\ d_1 \ \mathsf{alt}\ d_2\ ]\!]^u) = \pi_1.([\![\ d_1' \ \mathsf{alt}\ d_2'\ ]\!]^u) \cup \pi_2.([\![\ d_1' \ \mathsf{alt}\ d_2'\ ]\!]^u)$

⟨3⟩1. LET: $(p_i, n_i) = [\![\ d_i\ ]\!]$ and $(p_i', n_i') = [\![\ d_i'\ ]\!]$ for $i \in \{1, 2\}$

⟨3⟩2. $p_1 \cup n_1 = p_1' \cup n_1' \wedge p_2 \cup n_2 = p_2' \cup n_2'$
PROOF: By assumption ⟨1⟩1

⟨3⟩3. $(p_1 \cup p_2) \cup (n_1 \cup n_2) = (p_1' \cup p_2') \cup (n_1' \cup n_2')$
PROOF: By ⟨3⟩2

⟨3⟩4. Q.E.D.
PROOF: By ⟨3⟩3 and definition (9) in [RRS07]

⟨2⟩3. Q.E.D.
PROOF: By ⟨2⟩1 and ⟨2⟩2

⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

## C.2 Specifications with probabilistic choice

In this section $[\![\ \ldots\ ]\!]$ is always interpreted as $[\![\ \ldots\ ]\!]^p$, and $\langle I \rangle_d$ as $\langle I \rangle_d^p$.

### General lemmas

**Lemma 1.** *Let $O$ and $O'$ be sets of p-obligations. Then*

$$O \rightsquigarrow_{pl} O' \Rightarrow \oplus O \rightsquigarrow_r \oplus O'$$

PROOF.

⟨1⟩1. ASSUME: $O \rightsquigarrow_{pl} O'$
PROVE: $\oplus O \rightsquigarrow_r \oplus O'$

⟨2⟩1. ASSUME: $\oplus O \not\rightsquigarrow_r \oplus O'$
PROVE: $\bot$

⟨3⟩1. LET: $\oplus O = (p, n)$ and $\oplus O' = (p', n')$

⟨3⟩2. $n \not\subseteq n' \vee p \not\subseteq p' \cup n'$
PROOF: By assumption ⟨2⟩1

⟨3⟩3. CASE: $n \not\subseteq n'$

⟨4⟩1. LET: $t \in \mathcal{H}$ such that $t \in n \wedge t \notin n'$
PROOF: By assumption ⟨3⟩3

⟨4⟩2. LET: $((p_1', n_1'), Q_1') \in O'$ such that $t \notin n_1'$
PROOF: By ⟨4⟩1 and definition 4

⟨4⟩3. $\forall S \subseteq O' : ((p_1', n_1'), Q_1') \in S \Rightarrow t \notin \pi_2. \oplus S$
PROOF: By ⟨4⟩2

⟨4⟩4. $\forall((p_1, n_1), Q_1) \in O : t \in n_1$

PROOF: By $\langle 4\rangle 1$ and definition 4

$\langle 4\rangle 5.$ $\forall ((p_1, n_1), Q_1) \in O, S \subseteq O' : ((p_1', n_1'), Q_1') \in S \Rightarrow (p_1, n_1) \not\rightsquigarrow_r \oplus S$

PROOF: By $\langle 4\rangle 3$ and $\langle 4\rangle 4$

$\langle 4\rangle 6.$ Q.E.D.

PROOF: By assumption $\langle 1\rangle 1$ and $\langle 4\rangle 5$

$\langle 3\rangle 4.$ CASE: $p \not\subseteq p' \cup n'$

$\langle 4\rangle 1.$ LET: $t \in \mathcal{H}$ such that $t \in p \wedge t \notin p' \cup n'$

PROOF: By assumption $\langle 3\rangle 4$

$\langle 4\rangle 2.$ LET: $((p_1', n_1'), Q_1') \in O'$ such that $t \notin p_1' \cup n_1'$

PROOF: By $\langle 4\rangle 1$ and definition 4

$\langle 4\rangle 3.$ $\forall S \subseteq O' : ((p_1', n_1'), Q_1') \in S \Rightarrow t \notin \pi_1. \oplus S \cup \pi_2. \oplus S$

PROOF: By $\langle 4\rangle 2$ and definition 4

$\langle 4\rangle 4.$ $\forall ((p_1, n_1), Q_1) \in O : t \in p_1 \cup n_1$

PROOF: By $\langle 4\rangle 1$ and definition 4

$\langle 4\rangle 5.$ $\forall ((p_1, n_1), Q_1) \in O, S \subseteq O' : ((p_1', n_1'), Q_1') \in S \Rightarrow (p_1, n_1) \not\rightsquigarrow_r \oplus S$

PROOF: By $\langle 4\rangle 3$ and $\langle 4\rangle 4$

$\langle 4\rangle 6.$ Q.E.D.

PROOF: By By assumption $\langle 1\rangle 1$, definition 25 and $\langle 4\rangle 5$

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

PROOF: By $\langle 3\rangle 2$ the cases $\langle 3\rangle 3$ and $\langle 3\rangle 4$ are exhaustive

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

PROOF: $\perp$-rule

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

PROOF: $\Rightarrow$-rule

□

**Lemma 2.** *Let $d \in \mathcal{D}^p$. Then*

$$\pi_2.\bar{\oplus}[\![\ d\ ]\!] \subseteq \{1\}$$

PROOF.

$\langle 1\rangle 1.$ $\exists po \in [\![\ d\ ]\!] : Q \subseteq \{1\}$

$\langle 2\rangle 1.$ CASE: d consists of a single event $e$ or $d = \mathsf{skip}$

$\langle 3\rangle 1.$ $[\![\ d\ ]\!] = \{((\{\langle e\rangle\}, \emptyset), \{1\})\} \vee [\![\ d\ ]\!] = \{((\{\langle\rangle\}, \emptyset), \{1\})\}$

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

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

PROOF: By $\langle 3\rangle 1$

$\langle 2\rangle 2.$ CASE: $d$ contains at least one operator

$\langle 3\rangle 1.$ ASSUME: For every sequence diagram $d'$ that occur in an operand of $d$ the following holds: $\exists po' \in [\![\ d'\ ]\!] : Q' \subseteq \{1\}$ (ind. hyp.)

PROVE: $\exists po \in [\![\ d\ ]\!] : Q \subseteq \{1\}$

$\langle 4\rangle 1.$ CASE: $d = \mathsf{palt}(d_1;Q_1, \ldots d_n;Q_n)$

$\langle 5\rangle 1.$ $\exists po \in [\![\ d\ ]\!] : \pi_2.po = \{1\} \cap \sum_{i=1}^{n} Q_i$

PROOF: By $\langle 4\rangle 1$ and definition 9

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

PROOF: By $\langle 5\rangle 1$ and definition 7

$\langle 4\rangle 2.$ Case: $d = d_1 \ \mathsf{seq} \ d_2$

$\langle 5\rangle 1.$ Let: $po_1 \in [\![ \ d_1 \ ]\!]$ s.t. $Q_1 \subseteq \{1\}$
$po_2 \in [\![ \ d_2 \ ]\!]$ s.t. $Q_2 \subseteq \{1\}$

Proof: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ $po_1 \succsim po_2 \in [\![ \ d \ ]\!]$

Proof: By $\langle 5\rangle 1$ and assumption $\langle 4\rangle 2$

$\langle 5\rangle 3.$ $\pi_2.(po_1 \succsim po_2) \subseteq \{1\}$

Proof: By $\langle 5\rangle 1$

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

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 3$

$\langle 4\rangle 3.$ Case: $d = d_1 \ \mathsf{par} \ d_2$

Proof: Similar to $\langle 4\rangle 2$

$\langle 4\rangle 4.$ Case: $d = d_1 \ \mathsf{alt} \ d_2$

Proof: Similar to $\langle 4\rangle 2$

$\langle 4\rangle 5.$ Case: $d = \mathsf{refuse} \ d_1$

$\langle 5\rangle 1.$ Let: $(o, Q) \in [\![ \ d_1 \ ]\!]$ s.t. $Q \subseteq \{1\}$

Proof: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ $(\dagger o, Q) \in [\![ \ d \ ]\!]$

Proof: By $\langle 5\rangle 1$ and assumption $\langle 4\rangle 5$

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

Proof: By $\langle 5\rangle 1$ ($Q \subseteq \{1\}$) and $\langle 5\rangle 2$

$\langle 4\rangle 6.$ Q.E.D.

Proof: The cases $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$ and $\langle 4\rangle 5$ are exhaustive

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

Proof: Induction step

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

Proof: Induction with $\langle 2\rangle 1$ as base case and $\langle 2\rangle 2$ as induction step

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

Proof: By $\langle 1\rangle 1$, Definition 6 and Definition 7

□

**Lemma 3 (Monotonicity of $\succsim$, $\|$ and $\uplus$ w.r.t $\rightsquigarrow_{pr}$ for p-obligations).** *Let $(o_1, Q_1)$, $(o_2, Q_2)$, $(o_1', Q_1')$ and $(o_2', Q_2')$ be p-obligations. Then*

$$\begin{gathered}(o_1, Q_1) \rightsquigarrow_{pr} (o_1', Q_1') \wedge (o_2, Q_2) \rightsquigarrow_{pr} (o_2', Q_2') \Rightarrow \\ (o_1, Q_1) \succsim (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \succsim (o_2', Q_2') \wedge \\ (o_1, Q_1) \parallel (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \parallel (o_2', Q_2') \wedge \\ (o_1, Q_1) \uplus (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \uplus (o_2', Q_2')\end{gathered}$$

Proof.

$\langle 1\rangle 1.$ Assume: $(o_1, Q_1) \rightsquigarrow_{pr} (o_1', Q_1') \wedge (o_2, Q_2) \rightsquigarrow_{pr} (o_2', Q_2')$
Prove: $(o_1, Q_1) \succsim (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \succsim (o_2', Q_2') \wedge$
$(o_1, Q_1) \parallel (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \parallel (o_2', Q_2') \wedge$
$(o_1, Q_1) \uplus (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \uplus (o_2', Q_2')$

$\langle 2\rangle 1.$ $Q_1' * Q_2' \subseteq Q_1 * Q_2$

⟨3⟩1. $Q_1' \subseteq Q_1 \wedge Q_2' \subseteq Q_2$

Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1 and definition 2

⟨2⟩2. $(o_1, Q_1) \succsim (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \succsim (o_2', Q_2')$

⟨3⟩1. $o_1 \succsim o_2 \rightsquigarrow_r o_1' \succsim o_2'$

Proof: By assumption ⟨1⟩1 and Lemma 30 in [HHRS06]

⟨3⟩2. Q.E.D.

Proof: By ⟨2⟩1 and ⟨3⟩1

⟨2⟩3. $(o_1, Q_1) \parallel (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \parallel (o_2', Q_2')$

⟨3⟩1. $o_1 \parallel o_2 \rightsquigarrow_r o_1' \parallel o_2'$

Proof: By assumption ⟨1⟩1 and Lemma 31 in [HHRS06]

⟨3⟩2. Q.E.D.

Proof: By ⟨2⟩1 and ⟨3⟩1

⟨2⟩4. $(o_1, Q_1) \uplus (o_2, Q_2) \rightsquigarrow_{pr} (o_1', Q_1') \uplus (o_2', Q_2')$

⟨3⟩1. $o_1 \uplus o_2 \rightsquigarrow_r o_1' \uplus o_2'$

Proof: By assumption ⟨1⟩1 and Theorem 11 in [RRS07]

⟨3⟩2. Q.E.D.

Proof: By ⟨2⟩1 and ⟨3⟩1

⟨2⟩5. Q.E.D.

Proof: By ⟨2⟩2, ⟨2⟩3 and ⟨2⟩4

⟨1⟩2. Q.E.D.

Proof: ⇒-rule

□

**Lemma 4.** *Let $O_1$ and $O_2$ be sets of p-obligations. Then*

$$\oplus O_1 \succsim \oplus O_2 \rightsquigarrow_r \oplus(O_1 \succsim O_2)$$

Proof. In this proof we introduce the predicate $I$ defined by

$$I(t, t_1, t_2) \Leftrightarrow t \in \{t_1\} \succsim \{t_2\}$$

⟨1⟩1. $\pi_2.(\oplus O_1 \succsim \oplus O_2) \subseteq \pi_2. \oplus (O_1 \succsim O_2)$

⟨2⟩1. $\pi_2. \oplus (O_1 \succsim O_2) =$

$\{t \in \mathcal{H} \mid \forall po_1 \in O_1, po_2 \in O_2 : \exists t_1, t_2 \in \mathcal{H} : I(t, t_1, t_2) \wedge$
$(t_1 \in n_1 \wedge t_2 \in p_2) \vee$
$(t_1 \in p_1 \wedge t_2 \in n_2) \vee$
$(t_1 \in n_1 \wedge t_2 \in n_2)\}$

Proof: $\pi_2.\oplus(O_1 \succsim O_2)$

$= \bigcap_{po \in O_1 \succsim O_2} n$

By definition 4

$= \bigcap_{(po_1,po_2) \in O_1 \times O_2} n_1 \succsim p_2 \cup p_1 \succsim n_2 \cup n_1 \succsim n_2$

By definition 46 and definition (4) in [RRS07]

$= \bigcap_{(po_1,po_2) \in O_1 \times O_2} (\{t \in \mathcal{H} \mid \exists t_1 \in n_1, t_2 \in p_2 : I(t, t_1, t_2)\} \cup$

$\{t \in \mathcal{H} \mid \exists t_1 \in p_1, t_2 \in n_2 : I(t, t_1, t_2)\} \cup$

$\{t \in \mathcal{H} \mid \exists t_1 \in n_1, t_2 \in n_2 : I(t, t_1, t_2)\})$

By definition (2) in [RRS07]

$= \{t \in \mathcal{H} \mid \forall po_1 \in O_1, po_2 \in O_2 :$

$\exists t_1 \in n_1, t_2 \in p_2 : I(t, t_1, t_2) \vee$

$\exists t_1 \in p_1, t_2 \in n_2 : I(t, t_1, t_2) \vee$

$\exists t_1 \in n_1, t_2 \in n_2 : I(t, t_1, t_2)\}$

By set theory

$=$ righthand side of $\langle 2 \rangle 1$

$\langle 2 \rangle 2.$ $\pi_2.(\oplus O_1 \succsim \oplus O_2) =$

$\{t \in \mathcal{H} \mid \exists t_1, t_2 \in \mathcal{H} : I(t, t_1, t_2) \wedge$

$((\forall po_1 \in O_1 : t_1 \in n_1 \wedge \exists po_2 \in O_2 : t_2 \in p_2 \wedge \forall po_2' \in O_2 : t_2 \in p_2' \cup n_2') \vee$

$(\exists po_1 \in O_1 : t_1 \in p_1 \wedge \forall po_1' \in O_1 : t_1 \in p_1' \cup n_1' \wedge \forall po_2 \in O_2 : t_2 \in n_2) \vee$

$(\forall po_1 \in O_1 : t_1 \in n_1 \wedge \forall po_2 \in O_2 : t_2 \in n_2))\}$

Proof: $\pi_2.(\oplus O_1 \succsim \oplus O_2)$

$= \pi_2.\oplus O_1 \succsim \pi_1.\oplus O_2 \cup \pi_1.\oplus O_1 \succsim \pi_2.\oplus O_2 \cup \pi_2.\oplus O_1 \succsim \pi_2.\oplus O_2$

By Definition (4) in [RRS07]

$= \bigcap_{po_1 \in O_1} n_1 \succsim (\bigcup_{po_2 \in O_2} p_2 \cap \bigcap_{po_2 \in O_2} p_2 \cup n_2) \cup$

$(\bigcup_{po_1 \in O_1} p_1 \cap \bigcap_{po_1 \in O_1} p_1 \cup n_1) \succsim \bigcap_{po_2 \in O_2} n_2 \cup$

$\bigcap_{po_1 \in O_1} n_1 \succsim \bigcap_{po_2 \in O_2} n_2$

By definition 4

$=$ righthand side of $\langle 2 \rangle 2$

$\langle 2 \rangle 3.$ Assume: $t \in \pi_2.(\oplus O_1 \succsim \oplus O_2)$

Prove: $t \in \pi_2.\oplus(O_1 \succsim O_2)$

$\langle 3 \rangle 1.$ $\forall po_1 \in O_1, po_2 \in O_2 : \exists t_1, t_2 \in \mathcal{H} : I(t, t_1, t_2) \wedge$

$((t_1 \in n_1 \wedge t_2 \in p_2) \vee (t_1 \in p_1 \wedge t_2 \in n_2) \vee (t_1 \in n_1 \wedge t_2 \in n_2))$

$\langle 4 \rangle 1.$ Assume: $po_1 \in O_1, po_2 \in O_2$

Prove: $\exists t_1, t_2 \in \mathcal{H} : I(t, t_1, t_2) \wedge$

$((t_1 \in n_1 \wedge t_2 \in p_2) \vee$

$(t_1 \in p_1 \wedge t_2 \in n_2) \vee$

$(t_1 \in n_1 \wedge t_2 \in n_2))$

$\langle 5 \rangle 1.$ $\exists t_1', t_2' \in \mathcal{H} : I(t, t_1', t_2') \wedge$

$(\forall po_1' \in O_1 : t_1' \in n_1' \wedge \exists po_2' \in O_2 : t_2' \in p_2' \wedge$

$\forall po_2' \in O_2 : t_2' \in p_2' \cup n_2') \vee$

$(\exists po_1' \in O_1 : t_1' \in p_1' \wedge \forall po_1' \in O_1 : t_1' \in p_1' \cup n_1' \wedge$

$\forall po'_2 \in O_2 : t'_2 \in n'_2) \vee$
$(\forall po'_1 \in O_1 : t'_1 \in n'_1 \wedge \forall po'_2 \in O_2 : t'_2 \in n'_2)$

Proof: By ⟨2⟩2 and assumption ⟨2⟩3

⟨5⟩2. Case: $\forall po'_1 \in O_1 : t'_1 \in n'_1 \wedge \exists po'_2 \in O_2 : t'_2 \in p'_2 \wedge$
$\forall po'_2 \in O_2 : t'_2 \in p'_2 \cup n'_2$

⟨6⟩1. $t'_1 \in n_1 \wedge t'_2 \in p_2 \cup n_2$

Proof: By assumption ⟨5⟩2 and ⟨4⟩1

⟨6⟩2. $(t'_1 \in n_1 \wedge t'_2 \in p_2) \vee (t'_1 \in n_1 \wedge t_2 \in n_2)$

Proof: By ⟨6⟩1

⟨6⟩3. $I(t, t'_1, t'_2) \wedge$
$((t'_1 \in n_1 \wedge t'_2 \in p_2) \vee (t'_1 \in p_1 \wedge t'_2 \in n_2) \vee (t'_1 \in n_1 \wedge t'_2 \in n_2))$

Proof: By ⟨5⟩1 and ⟨6⟩2

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩3

⟨5⟩3. Case: $\exists po'_1 \in O_1 : t'_1 \in p'_1 \wedge \forall po'_1 \in O_1 : t'_1 \in p'_1 \cup n'_1 \wedge$
$\forall po'_2 \in O_2 : t'_2 \in n'_2$

⟨6⟩1. $t'_1 \in p_1 \cup n_1 \wedge t'_2 \in n_2$

Proof: By ⟨5⟩3 and ⟨4⟩1

⟨6⟩2. $(t'_1 \in p_1 \wedge t'_2 \in n_2) \vee (t'_1 \in n_1 \wedge t'_2 \in n_2)$

Proof: By ⟨6⟩1

⟨6⟩3. $I(t, t'_1, t'_2) \wedge$
$((t'_1 \in p_1 \wedge t'_2 \in n_2) \vee (t'_1 \in n_1 \wedge t'_2 \in p_2) \vee (t'_1 \in n_1 \wedge t'_2 \in n_2))$

Proof: By ⟨5⟩1 and ⟨6⟩2

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩3

⟨5⟩4. Case: $\forall po'_1 \in O_1 : t'_1 \in n'_1 \wedge \forall po'_2 \in O_2 : t'_2 \in n'_2$

⟨6⟩1. $t'_1 \in n_1 \wedge t'_2 \in n_2$

Proof: By assumption ⟨5⟩4 and ⟨4⟩1

⟨6⟩2. $(t'_1 \in n_1 \wedge t'_2 \in p_2) \vee (t'_1 \in p_1 \wedge t'_2 \in n_2) \vee (t'_1 \in n_1 \wedge t'_2 \in n_2)$

Proof: By ⟨6⟩1 (∨-intro)

⟨6⟩3. $I(t, t'_1, t'_2) \wedge$
$((t'_1 \in n_1 \wedge t'_2 \in p_2) \vee (t'_1 \in p_1 \wedge t'_2 \in n_2) \vee (t'_1 \in n_1 \wedge t'_2 \in n_2))$

Proof: By ⟨5⟩1 and ⟨6⟩2

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩3

⟨5⟩5. Q.E.D.

Proof: By ⟨5⟩1 the cases ⟨5⟩2, ⟨5⟩3 and ⟨5⟩4 are exhaustive

⟨4⟩2. Q.E.D.

Proof: ∀-rule

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1 and ⟨2⟩1

⟨2⟩4. Q.E.D.

Proof: ⊆-rule

⟨1⟩2. $\pi_1.(\oplus O_1 \succsim \oplus O_2) \subseteq \pi_1. \oplus (O_1 \succsim O_2) \cup \pi_2. \oplus (O_1 \succsim O_2)$

$\langle 2\rangle 1.$ $\pi_1.(\oplus O_1 \succsim \oplus O_2) =$
$\{t \in \mathcal{H} \mid \exists po_1 \in O_1, po_2 \in O_2, t_1 \in p_1, t_2 \in p_2 : I(t, t_1, t_2) \wedge$
$\forall po_1' \in O_1 : t_1 \in p_1' \cup n_1' \wedge \forall po_2' \in O_2 : t_2 \in p_2' \cup n_2'\}$

Proof: $\pi_1.(\oplus O_1 \succsim \oplus O_2)$

$= \pi_1. \oplus O_1 \succsim \pi_1. \oplus O_2$

By definition 50

$$= (\bigcup_{po_1 \in O_1} p_1 \cap (\bigcap_{po_1 \in O_1} p_1 \cup n_1)) \succsim (\bigcup_{po_2 \in O_2} p_2 \cap (\bigcap_{po_2 \in O_2} p_2 \cup n_2))$$

By definition 6

$= \{t_1 \in \mathcal{H} \mid \exists po_1 \in O_1 : t_1 \in p_1 \wedge \forall po_1' \in O_1 : t_1 \in p_1' \cup n_1'\} \succsim$
$\{t_2 \in \mathcal{H} \mid \exists po_2 \in O_2 : t_2 \in p_2 \wedge \forall po_2' \in O_2 : t_2 \in p_2' \cup n_2'\}$

By set theory

$=$ righthand side of $\langle 2\rangle 1$

By definition (2) in [RRS07]

$\langle 2\rangle 2.$ $\pi_1. \oplus (O_1 \succsim O_2) =$
$\{t \in \mathcal{H} \mid \exists po_1 \in O_1, po_2 \in O_2, t_1 \in p_1, t_2 \in p_2 : I(t, t_1, t_2) \wedge$
$\forall po_1' \in O_1, po_2' \in O_2 : \exists t_1' \in p_1' \cup n_1', t_2' \in p_2' \cup n_2' : I(t, t_1', t_2')\}$

Proof: $\pi_1. \oplus (O_1 \succsim O_2)$

$$= \bigcup_{po \in O_1 \succsim O_2} p \cap (\bigcap_{po \in O_1 \succsim O_2} p \cup n)$$

By definition 4

$= \{t \in \mathcal{H} \mid \exists po_1 \in O_1, po_2 \in O_2 : t_1 \in p_1, t_2 \in p_2 : I(t, t_1, t_2)\} \cap$
$\{t \in \mathcal{H} \mid \forall po_1 \in O_1, po_2 \in O_2 : \exists t_1 \in p_1 \cup n_1, t_2 \in p_2 \cup n_2 : I(t, t_1, t_2)\}$

By definition 46

$=$ righthand side of $\langle 2\rangle 2$

By set theory

$\langle 2\rangle 3.$ $\pi_1.(\oplus O_1 \succsim \oplus O_2) \subseteq \pi_1. \oplus (O_1 \succsim O_2)$

$\langle 3\rangle 1.$ Assume: $t \in \pi_1.(\oplus O_1 \succsim \oplus O_2)$
Prove: $t \in \pi_1. \oplus (O_1 \succsim O_2)$

$\langle 4\rangle 1.$ Assume: $t \notin \pi_1. \oplus (O_1 \succsim O_2)$
Prove: $\perp$

$\langle 5\rangle 1.$ $\exists po_1 \in O_1, po_2 \in O_2, t_1 \in p_1, t_2 \in p_2 : I(t, t_1, t_2) \wedge$
$\forall po_1' \in O_1 : t_1 \in p_1' \cup n_1' \wedge \forall po_2' \in O_2 : t_2 \in p_2' \cup n_2'$

Proof: By assumption $\langle 3\rangle 1$ and $\langle 2\rangle 1$

$\langle 5\rangle 2.$ $\neg(\exists po_1 \in O_1, po_2 \in O_2, t_1 \in p_1, t_2 \in p_2 : I(t, t_1, t_2) \wedge$
$\forall po_1' \in O_1, po_2' \in O_2 : \exists t_1' \in p_1' \cup n_1', t_2' \in p_2' \cup n_2' : I(t, t_1', t_2'))$

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

$\langle 5\rangle 3.$ $\forall po_1 \in O_1, po_2 \in O_2, t_1 \in p_1, t_2 \in p_2 : \neg I(t, t_1, t_2) \vee$
$\exists po_1' \in O_1, po_2' \in O_2 : \forall t_1' \in p_1' \cup n_1', t_2' \in p_2' \cup n_2' : \neg I(t, t_1', t_2')$

Proof: By $\langle 5\rangle 2$

$\langle 5\rangle 4.$ Case: $\forall po_1 \in O_1, po_2 \in O_2, t_1 \in p_1, t_2 \in p_2 : \neg I(t, t_1, t_2)$

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

Proof: By $\langle 5\rangle 1$ and $\langle 5\rangle 4$

$\langle 5\rangle 5.$ Case: $\exists po_1' \in O_1, po_2' \in O_2 :$
$\forall t_1' \in p_1' \cup n_1', t_2' \in p_2' \cup n_2' : \neg I(t, t_1', t_2')$

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

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 5$

$\langle 5\rangle 6$. Q.E.D.

PROOF: By $\langle 5\rangle 3$ the cases $\langle 5\rangle 4$ and $\langle 5\rangle 5$ are exhaustive

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

PROOF: $\bot$-rule

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

PROOF: $\subseteq$-rule

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

PROOF: By $\langle 2\rangle 3$

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

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

□

Note, however, that $\bar{\oplus} O_1 \succsim \bar{\oplus} O_2 \rightsquigarrow_{pr} \bar{\oplus}(O_1 \succsim O_2)$ does not in general hold, due to the probability sets. To see this, let

$$\begin{aligned} O_1 &= \{(o_a, \{0.2\})\} \\ O_2 &= \{(o_b, \langle 0.5, 1]), (o_c, \langle 0.5, 1])\} \end{aligned}$$

This means that

$$\begin{aligned} \bar{\oplus} O_1 &= (o_a, \{0.2\}) \\ \bar{\oplus} O_2 &= (\oplus\{o_b, o_c\}, \{1\}) \\ \pi_2.(\bar{\oplus} O_1 \succsim \bar{\oplus} O_2) &= \{0.2\} * \{1\} = \{0.2\} \\ \pi_2.\bar{\oplus}(O_1 \succsim O_2) &= \{0.2\} * \langle 0.5, 1] + \{0.2\} * \langle 0.5, 1] \\ &= \langle 0.1, 0.2] + \langle 0.1, 0.2] \\ &= \langle 0.2, 0.4] \end{aligned}$$

So $\pi_2.\bar{\oplus}(O_1 \succsim O_2) \not\subseteq \pi_2.\bar{\oplus} O_1 \succsim \bar{\oplus} O_2$.

Note also that neither $\oplus O_1 \succsim \oplus O_2 \rightsquigarrow_{rr} \oplus(O_1 \succsim O_2)$ nor $\oplus(O_1 \succsim O_2) \rightsquigarrow_{rr} \oplus O_1 \succsim \oplus O_2$ holds in general. To see this, let

$$\begin{aligned} O_1 &= \{((\{\langle a\rangle\}, \emptyset), Q_1), ((\{\langle ab\rangle\}, \emptyset), Q_2)\} \\ O_2 &= \{((\{\langle c\rangle, \langle bc\rangle\}, \emptyset), Q_3)\} \end{aligned}$$

This means that

$$\begin{aligned} O_1 \succsim O_2 &= \{((\{\langle ac\rangle, \langle abc\rangle\}, \emptyset), Q_1 * Q_3), ((\{\langle abc\rangle, \langle abbc\rangle\}, \emptyset), Q_2 * Q_3)\} \\ \oplus O_1 &= (\emptyset, \emptyset) \\ \oplus O_2 &= (\{\langle c\rangle, \langle bc\rangle\}, \emptyset) \\ \oplus(O_1 \succsim O_2) &= (\{\langle abc\rangle\}, \emptyset) \\ \oplus O_1 \succsim \oplus O_2 &= (\emptyset, \emptyset) \end{aligned}$$

So $\oplus O_1 \succsim \oplus O_2 \rightsquigarrow_{rr} \oplus(O_1 \succsim O_2)$ does not hold since $\langle abc\rangle$ is positive in $\oplus(O_1 \succsim O_2)$ but not in $\oplus O_1 \succsim \oplus O_2$, while $\oplus(O_1 \succsim O_2) \rightsquigarrow_{rr} \oplus O_1 \succsim \oplus O_2$ does not hold since $\langle abc\rangle$ is positive in $\oplus(O_1 \succsim O_2)$ but inconclusive in $\oplus O_1 \succsim \oplus O_2$.

**Lemma 5.** *Let $O_1$ and $O_2$ be sets of p-obligations. Then*

$$\oplus O_1 \parallel \oplus O_2 \rightsquigarrow_r \oplus(O_1 \parallel O_2)$$

Proof. Similar to Lemma 4; just replace $\succsim$ with $\parallel$. □

**Lemma 6.** *Let $O_1$ and $O_2$ be sets of p-obligations. Then*

$$\oplus O_1 \uplus \oplus O_2 \rightsquigarrow_r \oplus(O_1 \uplus O_2)$$

Proof.

⟨1⟩1. $\pi_1.(\oplus O_1 \uplus \oplus O_2) = \pi_1.\oplus O_1 \cup \pi_1.\oplus O_2 = (\bigcup_{po_1 \in O_1} p_1 \cap \bigcap_{po_1 \in O_1}(p_1 \cup n_1)) \cup (\bigcup_{po_2 \in O_2} p_2 \cap \bigcap_{po_2 \in O_2}(p_2 \cup n_2))$
Proof: By definition 4 and definition 51

⟨1⟩2. $\pi_2.(\oplus O_1 \uplus \oplus O_2) = \pi_2. \oplus O_1 \cup \pi_2. \oplus O_2 = \bigcap_{po_1 \in O_1} n_1 \cup \bigcap_{po_2 \in O_2} n_2$
Proof: By definition 4 and definition 51

⟨1⟩3. $\pi_2.(\oplus O_1 \uplus \oplus O_2) \subseteq \pi_2. \oplus (O_1 \uplus O_2)$
  ⟨2⟩1. Assume: $t \in \pi_2.(\oplus O_1 \uplus \oplus O_2)$
    Prove: $t \in \pi_2. \oplus (O_1 \uplus O_2)$
    ⟨3⟩1. $t \in \bigcap_{po_1 \in O_1} n_1 \vee t \in \bigcap_{po_2 \in O_2} n_2$
      Proof: By assumption ⟨2⟩1 and ⟨1⟩2
    ⟨3⟩2. Case: $t \in \bigcap_{po_1 \in O_1} n_1$
      ⟨4⟩1. $t \in \bigcap_{po \in O_1 \uplus O_2} n$
        Proof: By assumption ⟨3⟩2 and definition 47
      ⟨4⟩2. Q.E.D.
        Proof: By ⟨4⟩1 and definition 4
    ⟨3⟩3. Case: $t \in \bigcap_{po_2 \in O_2} n_2$
      Proof: Similar to ⟨3⟩2
    ⟨3⟩4. Q.E.D.
      Proof: By ⟨3⟩1 the cases ⟨3⟩2 and ⟨3⟩3 are exhaustive.
  ⟨2⟩2. Q.E.D.
    Proof: $\subseteq$-rule

⟨1⟩4. $\pi_1.(\oplus O_1 \uplus \oplus O_2) \subseteq \pi_1. \oplus (O_1 \uplus O_2) \cup \pi_2. \oplus (O_1 \uplus O_2)$
  ⟨2⟩1. Assume: $t \in \pi_1.(\oplus O_1 \uplus \oplus O_2)$
    Prove: $t \in \pi_1. \oplus (O_1 \uplus O_2) \cup \pi_2. \oplus (O_1 \uplus O_2)$
    ⟨3⟩1. $t \in (\bigcup_{po_1 \in O_1} p_1 \cap \bigcap_{po_1 \in O_1}(p_1 \cup n_1)) \vee t \in (\bigcup_{po_2 \in O_2} p_2 \cap \bigcap_{po_2 \in O_2}(p_2 \cup n_2))$
      Proof: By assumption ⟨2⟩1 and ⟨1⟩1
    ⟨3⟩2. Case: $t \in \bigcup_{po_1 \in O_1} p_1 \cap \bigcap_{po_1 \in O_1}(p_1 \cup n_1)$
      ⟨4⟩1. $t \in \bigcup_{po \in O_1 \uplus O_2} p$
        Proof: By assumption ⟨3⟩2 ($t \in \bigcup_{po_1 \in O_1} p_1$) and definition 47
      ⟨4⟩2. $t \in \bigcap_{po \in O_1 \uplus O_2}(p \cup n)$
        Proof: By assumption ⟨3⟩2 ($t \in \bigcap_{po_1 \in O_1} p_1 \cup n_1$) and definition 47
      ⟨4⟩3. $t \in \bigcup_{po \in O_1 \uplus O_2} p \cap \bigcap_{po \in O_1 \uplus O_2}(p \cup n)$
        Proof: By ⟨4⟩1 and ⟨4⟩2
      ⟨4⟩4. $t \in \pi_1. \oplus (O_1 \uplus O_2)$
        Proof: By ⟨4⟩3 and definition 4

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

Proof: By $\langle 4\rangle 4$

$\langle 3\rangle 3.$ Case: $t \in (\bigcup_{po_2 \in O_2} p_2 \cap \bigcap_{po_2 \in O_2}(p_2 \cup n_2))$

Proof: Similar to $\langle 3\rangle 2$

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

Proof: By $\langle 3\rangle 1$ the cases $\langle 3\rangle 2$ and $\langle 3\rangle 3$ are exhaustive.

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

Proof: $\subseteq$-rule

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

Proof: By $\langle 1\rangle 3$ and $\langle 1\rangle 4$

□

**Lemma 7.** *Let $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^p$, and let $op \in \{\succsim, \|, \uplus\}$. Then*

$$\pi_2.(\bar{\oplus}[\![\ d_1\ ]\!]\ op\ \bar{\oplus}[\![\ d_2\ ]\!]) = \pi_2.\bar{\oplus}([\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!])$$

Proof.

$\langle 1\rangle 1.$ $\pi_2.\bar{\oplus}[\![\ d_1\ ]\!] \subseteq \{1\} \wedge \pi_2.\bar{\oplus}[\![\ d_2\ ]\!] \subseteq \{1\}$

Proof: By Lemma 2

$\langle 1\rangle 2.$ $\pi_2.(\bar{\oplus}[\![\ d_1\ ]\!]\ op\ \bar{\oplus}[\![\ d_2\ ]\!]) \subseteq \{1\}$

Proof: By $\langle 1\rangle 1$

$\langle 1\rangle 3.$ $\pi_2.\bar{\oplus}([\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!]) \subseteq \{1\}$

Proof: By Lemma 2

$\langle 1\rangle 4.$ $1 \in \pi_2.(\bar{\oplus}[\![\ d_1\ ]\!]\ op\ \bar{\oplus}[\![\ d_2\ ]\!]) \Rightarrow 1 \in \pi_2.\bar{\oplus}([\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!])$

$\langle 2\rangle 1.$ Assume: $1 \in \pi_2.(\bar{\oplus}[\![\ d_1\ ]\!]\ op\ \bar{\oplus}[\![\ d_2\ ]\!])$
Prove: $1 \in \pi_2.\bar{\oplus}([\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!])$

$\langle 3\rangle 1.$ $\pi_2.\bar{\oplus}[\![\ d_1\ ]\!] \neq \emptyset \wedge \pi_2.\bar{\oplus}[\![\ d_2\ ]\!] \neq \emptyset$

Proof: By assumption $\langle 2\rangle 1$

$\langle 3\rangle 2.$ $1 \in \pi_2.\bar{\oplus}[\![\ d_1\ ]\!] \wedge 1 \in \pi_2.\bar{\oplus}[\![\ d_2\ ]\!]$

Proof: By $\langle 1\rangle 1$ and $\langle 3\rangle 1$

$\langle 3\rangle 3.$ Assume: $1 \notin \pi_2.\bar{\oplus}([\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!])$
Prove: $\perp$

$\langle 4\rangle 1.$ $\pi_2.\bar{\oplus}([\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!]) = \emptyset$

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

$\langle 4\rangle 2.$ $\exists po_1 \in [\![\ d_1\ ]\!] : \pi_2.po_1 = \emptyset \vee \exists po_2 \in [\![\ d_2\ ]\!] : \pi_2.po_2 = \emptyset$

$\langle 5\rangle 1.$ $\exists po \in [\![\ d_1\ ]\!]\ op\ [\![\ d_2\ ]\!] : \pi_2.po = \emptyset$

Proof: By $\langle 4\rangle 1$

$\langle 5\rangle 2.$ Let: $po_1 \in [\![\ d_1\ ]\!], po_2 \in [\![\ d_2\ ]\!]$ s.t. $\pi_2.(po_1\ op\ po_2) = \emptyset$

Proof: By $\langle 5\rangle 1$

$\langle 5\rangle 3.$ $\pi_2.po_1 * \pi_2.po_2 = \emptyset$

Proof: By $\langle 5\rangle 2$

$\langle 5\rangle 4.$ $\pi_2.po_1 = \emptyset \vee \pi_2.po_2 = \emptyset$

Proof: By $\langle 5\rangle 3$

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

Proof: By $\langle 5\rangle 4$ and $\langle 5\rangle 2$

$\langle 4\rangle 3.$ Case: $\exists po_1 \in [\![\ d_1\ ]\!] : \pi_2.po_1 = \emptyset$

⟨5⟩1. $\pi_2.\bar{\oplus}\llbracket\, d_1 \,\rrbracket = \emptyset$

PROOF: By assumption ⟨4⟩3, definition 6 and definition 7

⟨5⟩2. Q.E.D.

PROOF: By ⟨3⟩2 and ⟨5⟩1

⟨4⟩4. CASE: $\exists po_2 \in \llbracket\, d_2 \,\rrbracket : \pi_2.po_2 = \emptyset$

PROOF: Similar to case ⟨4⟩3

⟨4⟩5. Q.E.D.

PROOF: By ⟨4⟩2 the cases ⟨4⟩3 and ⟨4⟩4 are exhaustive

⟨3⟩4. Q.E.D.

PROOF: ⊥-rule (⟨3⟩3)

⟨2⟩2. Q.E.D.

PROOF: ⇒-rule

⟨1⟩5. $1 \in \pi_2.\bar{\oplus}(\llbracket\, d_1 \,\rrbracket\ op\ \llbracket\, d_2 \,\rrbracket) \Rightarrow 1 \in \pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket\ op\ \bar{\oplus}\llbracket\, d_2 \,\rrbracket)$

⟨2⟩1. ASSUME: $1 \in \pi_2.\bar{\oplus}(\llbracket\, d_1 \,\rrbracket\ op\ \llbracket\, d_2 \,\rrbracket)$

PROVE: $1 \in \pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket\ op\ \bar{\oplus}\llbracket\, d_2 \,\rrbracket)$

⟨3⟩1. ASSUME: $1 \notin \pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket\ op\ \bar{\oplus}\llbracket\, d_2 \,\rrbracket)$

PROVE: $\bot$

⟨4⟩1. $\pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket\ op\ \bar{\oplus}\llbracket\, d_2 \,\rrbracket) = \emptyset$

PROOF: By ⟨1⟩2 and assumption ⟨3⟩1

⟨4⟩2. $\pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket) = \emptyset \vee \pi_2.(\bar{\oplus}\llbracket\, d_2 \,\rrbracket) = \emptyset$

⟨5⟩1. $\pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket) * \pi_2.(\bar{\oplus}\llbracket\, d_2 \,\rrbracket) = \emptyset$

PROOF: By ⟨4⟩1

⟨5⟩2. Q.E.D.

PROOF: By ⟨5⟩1

⟨4⟩3. CASE: $\pi_2.(\bar{\oplus}\llbracket\, d_1 \,\rrbracket) = \emptyset$

⟨5⟩1. $\exists po_1 \in \llbracket\, d_1 \,\rrbracket : \pi_2.po_1 = \emptyset$

PROOF: By assumption ⟨4⟩3, definition 6 and definition 7

⟨5⟩2. $\exists po \in \llbracket\, d_1 \,\rrbracket\ op\ \llbracket\, d_2 \,\rrbracket : \pi_2.po = \emptyset$

PROOF: By ⟨5⟩1

⟨5⟩3. $\pi_2.\bar{\oplus}(\llbracket\, d_1 \,\rrbracket\ op\ \llbracket\, d_2 \,\rrbracket) = \emptyset$

PROOF: By ⟨5⟩2, definition 6 and definition 7

⟨5⟩4. Q.E.D.

PROOF: By ⟨5⟩3 and assumption ⟨2⟩1

⟨4⟩4. CASE: $\pi_2.(\bar{\oplus}\llbracket\, d_2 \,\rrbracket) = \emptyset$

PROOF: Similar to case ⟨4⟩3

⟨4⟩5. Q.E.D.

PROOF: By ⟨4⟩2, the cases ⟨4⟩3 and ⟨4⟩4 are exhaustive

⟨3⟩2. Q.E.D.

PROOF: ⊥-rule

⟨2⟩2. Q.E.D.

PROOF: ⇒-rule

⟨1⟩6. Q.E.D.

PROOF: By ⟨1⟩2, ⟨1⟩3, ⟨1⟩4 and ⟨1⟩5

□

**Lemma 8.** *Let $O$ be a set of p-obligations. Then*

$$\bar{\oplus}\dagger O = \dagger\bar{\oplus}O$$

Proof.

$\langle 1\rangle 1.$ $\pi_1.\bar{\oplus}\dagger O = \pi_1.\dagger\bar{\oplus}O$

Proof:

$$\begin{aligned}
\pi_1.\bar{\oplus}\dagger O &= \oplus\dagger O && \text{By definition 6}\\
&= (\textstyle\bigcup_{po\in\dagger O} p \cap \bigcap_{po\in\dagger O}(p\cup n), \bigcap_{po\in\dagger O} n) && \text{By definition 4}\\
&= (\emptyset, \textstyle\bigcap_{po\in O} p\cup n) && \text{By definition 48}\\
&= \dagger(\textstyle\bigcup_{po\in O} p \cap \bigcap_{po\in O}(p\cup n), \bigcap_{po\in O} n) && \text{By definition 52}\\
&= \dagger\oplus O && \text{By definition 4}\\
&= \pi_1.\dagger\bar{\oplus}O && \text{By definition 6}
\end{aligned}$$

$\langle 1\rangle 2.$ $\pi_2.\bar{\oplus}\dagger O = \pi_2.\dagger\bar{\oplus}O$

$\langle 2\rangle 1.$ $\pi_2.\bar{\oplus}\dagger O = \sum_{po\in\dagger O}\pi_2.po = \sum_{po\in O}\pi_2.po = \pi_2.\bar{\oplus}O = \pi_2.\dagger\bar{\oplus}O$

Proof: By definition 6, definition 48 and definition 52

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

Proof: By $\langle 2\rangle 1$

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

Proof: By $\langle 1\rangle 1$ and $\langle 1\rangle 2$

□

**Lemma 9.** *Let $(o, Q)$ and $(o', Q')$ be p-obligations. Then*

$$(o, Q) \rightsquigarrow_{pr} (o', Q') \Rightarrow \dagger(o, Q) \rightsquigarrow_{pr} \dagger(o', Q')$$

Proof.

$\langle 1\rangle 1.$ Assume: $(o, Q) \rightsquigarrow_{pr} (o', Q')$
Prove: $\dagger(o, Q) \rightsquigarrow_{pr} \dagger(o', Q')$

$\langle 2\rangle 1.$ $\dagger o \rightsquigarrow_r \dagger o'$

$\langle 3\rangle 1.$ $o \rightsquigarrow_r o'$

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

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

Proof: By $\langle 3\rangle 1$ and Lemma 4 in [RHS07b] (note that the proof of Lemma 4 in [RHS07b] applies for any interaction obligation).

$\langle 2\rangle 2.$ $Q' \subseteq Q$

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

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

Proof: By $\langle 2\rangle 1$ and $\langle 2\rangle 2$

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

Proof: $\Rightarrow$-rule

□

**Lemma 10.** *Let $O_i$ and $O'_i$ be sets of p-obligations. Then*

$$(\forall i \leq n : \oplus O_i \rightsquigarrow_r \oplus O'_i) \Rightarrow \oplus\bigcup_{i=1}^{n} O_i \rightsquigarrow_r \oplus\bigcup_{i=1}^{n} O'$$

Proof.

⟨1⟩1. Assume: $\forall i \leq n : \oplus O_i \rightsquigarrow_r \oplus O'_i$
Prove: $\oplus \bigcup_{i=1}^{n} O_i \rightsquigarrow_r \oplus \bigcup_{i=1}^{n} O'$

⟨2⟩1. Case: $n = 1$
(induction basis)

⟨3⟩1. $\oplus O_1 \rightsquigarrow_r \oplus O'_1$
Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.
Proof: By ⟨3⟩1

⟨2⟩2. Case: $n > 1$ (induction step)

⟨3⟩1. Assume: $\oplus \bigcup_{i=1}^{k} O_i \rightsquigarrow_r \oplus \bigcup_{i=1}^{k} O'$ for $k < n$ (ind. hyp.)
Prove: $\oplus \bigcup_{i=1}^{k+1} O_i \rightsquigarrow_r \oplus \bigcup_{i=1}^{k+1} O'$

⟨4⟩1. $O_{k+1} \rightsquigarrow_r \oplus O'_{k+1}$
Proof: By assumption ⟨1⟩1

⟨4⟩2. Q.E.D.
Proof: By ⟨4⟩1, assumption ⟨3⟩1 and Lemma 6 in [RHS07a]

⟨3⟩2. Q.E.D.
Proof: Induction step

⟨2⟩3. Q.E.D.
Proof: By induction with ⟨2⟩1 as basis and ⟨2⟩2 as induction step

⟨1⟩2. Q.E.D.
Proof: ⇒-rule

□

**Lemma 11.** *Let $d \in \mathcal{D}^p$. Then*

$$\exists po \in [\![ \ d \ ]\!] : po \rightsquigarrow_{pr} \bar{\oplus}[\![ \ d \ ]\!] \wedge Q \subseteq \{1\}$$

Proof.

⟨1⟩1. Case: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

⟨2⟩1. $[\![ \ d \ ]\!] = \{((\{\langle e \rangle\}, \emptyset), \{1\})\} = \{\bar{\oplus}[\![ \ d \ ]\!]\} \vee$
$[\![ \ d \ ]\!] = \{((\{\langle\rangle\}, \emptyset), \{1\})\} = \{\bar{\oplus}[\![ \ d \ ]\!]\}$
Proof: By assumption ⟨1⟩1

⟨2⟩2. Q.E.D.
Proof: By ⟨2⟩1 and reflexivity of $\rightsquigarrow_{pr}$

⟨1⟩2. Case: $d$ contains at least one operator

⟨2⟩1. Assume: For every sequence diagram $d'$ that occur in an operand of an operator in $d$ the following holds:
$\exists po' \in [\![ \ d' \ ]\!] : po' \rightsquigarrow_{pr} \bar{\oplus}[\![ \ d' \ ]\!] \wedge Q' \subseteq \{1\}$ (ind. hyp.).
Prove: $\exists po \in [\![ \ d \ ]\!] : po \rightsquigarrow_{pr} \bar{\oplus}[\![ \ d \ ]\!]$

⟨3⟩1. Case: $d = \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)$

⟨4⟩1. Let: $po_a = (\oplus \bigcup_{i=1}^{n} [\![ \ d_1;Q_i \ ]\!], \{1\} \cap \sum_{i=1}^{n} Q_i)$

⟨4⟩2. $po_a \in [\![ \ d \ ]\!]$
Proof: By assumption ⟨3⟩1 and definition 9

⟨4⟩3. $Q_a \subseteq \{1\}$

Proof: By ⟨4⟩1

⟨4⟩4. $po_a \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d\ \rrbracket$

⟨5⟩1. $\pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket \subseteq Q_a$

⟨6⟩1. $\pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket \subseteq \{1\}$

Proof: By Lemma 2

⟨6⟩2. Case: $\pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket = \{1\}$

⟨7⟩1. $1 \in \sum_{i=1}^{n} Q_i$

⟨8⟩1. Assume: $1 \notin \sum_{i=1}^{n} Q_i$
Prove: $\bot$

⟨9⟩1. $Q_a = \emptyset$

Proof: By ⟨4⟩1 and assumption ⟨8⟩1

⟨9⟩2. $\exists po \in \llbracket\ d\ \rrbracket : Q = \emptyset$

Proof: By ⟨9⟩1 and ⟨4⟩2

⟨9⟩3. $\pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket = \emptyset$

Proof: By ⟨9⟩2

⟨9⟩4. Q.E.D.

Proof: By ⟨9⟩3 and assumption ⟨6⟩2

⟨8⟩2. Q.E.D.

Proof: $\bot$-rule

⟨7⟩2. $1 \in Q_a$

Proof: By ⟨7⟩1 and ⟨4⟩1

⟨7⟩3. Q.E.D.

Proof: By ⟨7⟩2 and assumption ⟨6⟩2

⟨6⟩3. Case: $\pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket = \emptyset$

Proof: By assumption ⟨6⟩3

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩1, the cases ⟨6⟩2 and ⟨6⟩3 are exhaustive

⟨5⟩2. $o_a \rightsquigarrow_r \oplus\llbracket\ d\ \rrbracket$

⟨6⟩1. $\oplus\llbracket\ d\ \rrbracket = \oplus \bigcup_{i=1}^{n} \llbracket\ d_i;Q_i\ \rrbracket$

Proof: By assumption ⟨3⟩1

⟨6⟩2. $o_a = \oplus \bigcup_{i=1}^{n} \llbracket\ d_i;Q_i\ \rrbracket$

Proof: By ⟨4⟩1

⟨6⟩3. Q.E.D.

Proof: By ⟨6⟩1 and ⟨6⟩2

⟨5⟩3. Q.E.D.

Proof: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩5. Q.E.D.

Proof: By ⟨4⟩2, ⟨4⟩3 and ⟨4⟩4; $po_a$ is the *po* we are looking for.

⟨3⟩2. Case: $d = d_1$ seq $d_2$

⟨4⟩1. Let: $po_1 \in \llbracket\ d_1\ \rrbracket$ such that $po_1 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \wedge Q_1 \subseteq \{1\}$
$po_2 \in \llbracket\ d_2\ \rrbracket$ such that $po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_2\ \rrbracket \wedge Q_2 \subseteq \{1\}$

Proof: By assumption ⟨2⟩1

⟨4⟩2. $po_1 \succsim po_2 \in \llbracket\ d\ \rrbracket$

Proof: By ⟨4⟩1 and assumption ⟨3⟩2

⟨4⟩3. $\pi_2.(po_1 \succsim po_2) \subseteq \{1\}$

PROOF: By ⟨4⟩1

⟨4⟩4. $po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \succsim \bar{\oplus}\llbracket\ d_2\ \rrbracket$

PROOF: By ⟨4⟩1 and Lemma 3

⟨4⟩5. $\bar{\oplus}\llbracket\ d_1\ \rrbracket \succsim \bar{\oplus}\llbracket\ d_2\ \rrbracket \rightsquigarrow_{pr} \bar{\oplus}(\llbracket\ d_1\ \rrbracket \succsim \llbracket\ d_2\ \rrbracket)$

⟨5⟩1. $\oplus\llbracket\ d_1\ \rrbracket \succsim \oplus\llbracket\ d_2\ \rrbracket \rightsquigarrow_{r} \oplus(\llbracket\ d_1\ \rrbracket \succsim \llbracket\ d_2\ \rrbracket)$

PROOF: By Lemma 4

⟨5⟩2. $\pi_2.\bar{\oplus}(\llbracket\ d_1\ \rrbracket \succsim \llbracket\ d_2\ \rrbracket) \subseteq \pi_2.(\bar{\oplus}\llbracket\ d_1\ \rrbracket \succsim \bar{\oplus}\llbracket\ d_2\ \rrbracket)$

PROOF: By Lemma 7

⟨5⟩3. Q.E.D.

PROOF: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩6. $po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}(\llbracket\ d_1\ \rrbracket \succsim \llbracket\ d_2\ \rrbracket)$

PROOF: By ⟨4⟩4, ⟨4⟩5 and Lemma 1 in [RHS07a] (transitivity of $\rightsquigarrow_{pr}$)

⟨4⟩7. Q.E.D.

PROOF: By ⟨4⟩2, ⟨4⟩3 and ⟨4⟩6; $po_1 \succsim po_2$ is the $po$ we are looking for.

⟨3⟩3. CASE: $d = d_1\ \mathsf{par}\ d_2$

PROOF: Similar to case ⟨3⟩2, with $\succsim$ replaced by $\|$, and the reference to Lemma 4 replaced by a reference to Lemma 5.

⟨3⟩4. CASE: $d = d_1 \mathsf{alt}\ d_2$

⟨4⟩1. LET: $po_1 \in \llbracket\ d_1\ \rrbracket$ such that $po_1 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \wedge Q_1 \subseteq \{1\}$
$po_2 \in \llbracket\ d_2\ \rrbracket$ such that $po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_2\ \rrbracket \wedge Q_1 \subseteq \{1\}$

PROOF: By assumption ⟨2⟩1

⟨4⟩2. $po_1 \uplus po_2 \in \llbracket\ d\ \rrbracket$

PROOF: By ⟨4⟩1 and assumption ⟨3⟩4

⟨4⟩3. $\pi_2.(po_1 \uplus po_2) \subseteq \{1\}$

PROOF: By ⟨4⟩1

⟨4⟩4. $po_1 \uplus po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \uplus \bar{\oplus}\llbracket\ d_2\ \rrbracket$

PROOF: By ⟨4⟩1 and Lemma 3

⟨4⟩5. $\bar{\oplus}\llbracket\ d_1\ \rrbracket \uplus \bar{\oplus}\llbracket\ d_2\ \rrbracket \rightsquigarrow_{pr} \bar{\oplus}(\llbracket\ d_1\ \rrbracket \uplus \llbracket\ d_2\ \rrbracket)$

⟨5⟩1. $\oplus\llbracket\ d_1\ \rrbracket \uplus \oplus\llbracket\ d_2\ \rrbracket \rightsquigarrow_{r} \oplus(\llbracket\ d_1\ \rrbracket \uplus \llbracket\ d_2\ \rrbracket)$

PROOF: By Lemma 6

⟨5⟩2. $\pi_2.\bar{\oplus}(\llbracket\ d_1\ \rrbracket \uplus \llbracket\ d_2\ \rrbracket) \subseteq \pi_2.(\bar{\oplus}\llbracket\ d_1\ \rrbracket \uplus \bar{\oplus}\llbracket\ d_2\ \rrbracket)$

PROOF: By Lemma 7

⟨5⟩3. Q.E.D.

PROOF: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩6. $po_1 \uplus po_2 \rightsquigarrow_{pr} \bar{\oplus}(\llbracket\ d_1\ \rrbracket \uplus \llbracket\ d_2\ \rrbracket)$

PROOF: By ⟨4⟩4, ⟨4⟩5 and Lemma 1 in [RHS07a] (transitivity of $\rightsquigarrow_{pr}$)

⟨4⟩7. Q.E.D.

PROOF: By ⟨4⟩2, ⟨4⟩3 and ⟨4⟩6; $po_1 \uplus po_2$ is the $po$ we are looking for.

⟨3⟩5. CASE: $d = \mathsf{refuse}\ d_1$

⟨4⟩1. LET: $po_1 \in \llbracket\ d_1\ \rrbracket$ such that $po_1 \rightsquigarrow \llbracket\ d_1\ \rrbracket \wedge Q_1 \subseteq \{1\}$

PROOF: By assumption ⟨2⟩1

⟨4⟩2. $\dagger po_1 \in \llbracket\ d\ \rrbracket$

PROOF: By ⟨4⟩1 and assumption ⟨3⟩5

⟨4⟩3. $\pi_2.(\dagger po_1) \subseteq \{1\}$

PROOF: By ⟨4⟩1

$\langle 4\rangle 4.$ $\dagger po_1 \rightsquigarrow_{pr} \dagger\bar{\oplus}\llbracket\ d_1\ \rrbracket$
Proof: By $\langle 4\rangle 1$ and Lemma 9
$\langle 4\rangle 5.$ $\dagger po_1 \rightsquigarrow_{pr} \bar{\oplus}\dagger\llbracket\ d_1\ \rrbracket$
Proof: By $\langle 4\rangle 4$ and Lemma 8
$\langle 4\rangle 6.$ Q.E.D.
Proof: By $\langle 4\rangle 2$, $\langle 4\rangle 3$ and $\langle 4\rangle 5$; $\dagger po_1$ is the *po* we are looking for.
$\langle 3\rangle 6.$ Q.E.D.
Proof: The cases $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ and $\langle 3\rangle 5$ are exhaustive.
$\langle 2\rangle 2.$ Q.E.D.
Proof: Induction step
$\langle 1\rangle 3.$ Q.E.D.
Proof: By induction with $\langle 1\rangle 1$ as basis and $\langle 1\rangle 2$ as induction step

□

**Lemma 12.** *Let $d \in \mathcal{D}^p$. Then*

$$\exists po \in \llbracket\ d\ \rrbracket : po \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d\ \rrbracket \land Q \subseteq \{1\}$$

Proof.

$\langle 1\rangle 1.$ Let: $po_1 \in \llbracket\ d\ \rrbracket$ such that $po_1 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d\ \rrbracket \land Q_1 \subseteq \{1\}$
Proof: By Lemma 11
$\langle 1\rangle 2.$ Let: $po_1' = \bar{\oplus}\llbracket\ d\ \rrbracket$
$\langle 1\rangle 3.$ $p_1' \cup n_1' = p_1 \cup n_1$
$\langle 2\rangle 1.$ $p_1 \cup n_1 \subseteq p_1' \cup n_1'$
Proof: By $\langle 1\rangle 1$
$\langle 2\rangle 2.$ $p_1' \cup n_1' \subseteq p_1 \cup n_1$
$\langle 3\rangle 1.$ Assume: $t \in p_1' \cup n_1'$
Prove: $t \in p_1 \cup n_1$
$\langle 4\rangle 1.$ $\forall po \in \llbracket\ d\ \rrbracket : t \in p \cup n$
Proof: By assumption $\langle 3\rangle 1$
$\langle 4\rangle 2.$ Q.E.D.
Proof: By $\langle 4\rangle 1$ and $\langle 1\rangle 1$ ($po_1 \in \llbracket\ d\ \rrbracket$)
$\langle 3\rangle 2.$ Q.E.D.
Proof: $\subseteq$-rule
$\langle 2\rangle 3.$ Q.E.D.
Proof: By $\langle 2\rangle 1$ and $\langle 2\rangle 2$
$\langle 1\rangle 4.$ Q.E.D.
Proof: By $\langle 1\rangle 1$, $\langle 1\rangle 2$ and $\langle 1\rangle 3$; $po_1$ is the *po* we are looking for.

**Lemma 13.** *Let $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'\ \rrbracket \Rightarrow \oplus\llbracket\ d\ \rrbracket \rightsquigarrow_{nr} \oplus\llbracket\ d'\ \rrbracket$$

Proof.

$\langle 1\rangle 1.$ Assume: $\llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'\ \rrbracket$
Prove: $\oplus\llbracket\ d\ \rrbracket \rightsquigarrow_{nr} \oplus\llbracket\ d'\ \rrbracket$

$\langle 2\rangle 1.$ LET: $(p_1, n_1) = \oplus\llbracket\ d\ \rrbracket$
$(p'_1, n'_1) = \oplus\llbracket\ d'\ \rrbracket$

$\langle 2\rangle 2.$ $(p_1, n_1) \rightsquigarrow_r (p'_1, n'_1)$

$\langle 3\rangle 1.$ $\llbracket\ d\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d'\ \rrbracket$

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

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

PROOF: By $\langle 3\rangle 1$ and Lemma 1

$\langle 2\rangle 3.$ $p_1 \cup n_1 = p'_1 \cup n'_1$

$\langle 3\rangle 1.$ $p_1 \cup n_1 \subseteq p'_1 \cup n'_1$

PROOF: By $\langle 2\rangle 2$

$\langle 3\rangle 2.$ $p'_1 \cup n'_1 \subseteq p_1 \cup n_1$

$\langle 4\rangle 1.$ ASSUME: $t \in p'_1 \cup n'_1$
PROVE: $t \in p_1 \cup n_1$

$\langle 5\rangle 1.$ LET: $po_2 \in \llbracket\ d\ \rrbracket$ s.t. $po_2 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d\ \rrbracket \wedge Q_2 \subseteq \{1\}$

PROOF: By Lemma 12

$\langle 5\rangle 2.$ $0 \notin Q_2$

PROOF: By $\langle 5\rangle 1$

$\langle 5\rangle 3.$ LET: $po'_2 \in \llbracket\ d'\ \rrbracket$ s.t. $po_2 \rightsquigarrow_{pnr} po'_2$

PROOF: By $\langle 5\rangle 1$, $\langle 5\rangle 2$ and assumption $\langle 1\rangle 1$

$\langle 5\rangle 4.$ $t \in p'_2 \cup n'_2$

$\langle 6\rangle 1.$ $\forall po \in \llbracket\ d'\ \rrbracket : t \in p \cup n$

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

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

PROOF: By $\langle 6\rangle 1$ and $\langle 5\rangle 3$ ($po'_2 \in \llbracket\ d'\ \rrbracket$)

$\langle 5\rangle 5.$ $t \in p_2 \cup n_2$

PROOF: By $\langle 5\rangle 4$ and $\langle 5\rangle 3$

$\langle 5\rangle 6.$ $\forall po \in \llbracket\ d\ \rrbracket : t \in p \cup n$

$\langle 6\rangle 1.$ ASSUME: $\exists po \in \llbracket\ d\ \rrbracket : t \notin p \cup n$
PROVE: $\perp$

$\langle 7\rangle 1.$ $t \notin p_1 \cup n_1$

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

$\langle 7\rangle 2.$ $t \notin p_2 \cup n_2$

PROOF: By $\langle 7\rangle 1$ and $\langle 5\rangle 1$

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

PROOF: By $\langle 7\rangle 2$ and $\langle 5\rangle 5$

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

PROOF: $\perp$-rule

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

PROOF: By $\langle 5\rangle 6$

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

PROOF: $\subseteq$-rule

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

PROOF: By $\langle 3\rangle 1$ and $\langle 3\rangle 2$

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

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$ and $\langle 2\rangle 3$

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

**Lemma 14.** *Let $(o, Q)$ and $(o', Q')$ be p-obligations. Then*

$$(o, Q) \rightsquigarrow_{pnr} (o', Q') \Rightarrow \dagger(o, Q) \rightsquigarrow_{pnr} \dagger(o', Q')$$

PROOF. The proof is similar to the proof of Lemma 9; replace $\rightsquigarrow_{rr}$ with $\rightsquigarrow_{nr}$, $\rightsquigarrow_{pr}$ with $\rightsquigarrow_{pnr}$, and the reference to Lemma 4 in [RHS07b] with a reference to Theorem 7. □

**Lemma 15.** *Let $(o_1, Q_1)$, $(o_2, Q_2)$ and $(o_3, Q_3)$ be p-obligations. Then*

$$(o_1, Q_1) \rightsquigarrow_{prr} (o_2, Q_2) \wedge (o_2, Q_2) \mapsto_{prr} (o_3, Q_3) \Rightarrow (o_1, Q_1) \mapsto_{prr} (o_3, Q_3)$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $(o_1, Q_1) \rightsquigarrow_{prr} (o_2, Q_2) \wedge (o_2, Q_2) \mapsto_{prr} (o_3, Q_3)$
  PROVE: $(o_1, Q_1) \mapsto_{prr} (o_3, Q_3)$
  $\langle 2\rangle 1.$ $o_1 \mapsto_{rr} o_3$
    $\langle 3\rangle 1.$ $o_1 \rightsquigarrow_{rr} o_2 \wedge o_2 \mapsto_{rr} o_3$
      PROOF: By assumption $\langle 1\rangle 1$
    $\langle 3\rangle 2.$ Q.E.D.
      PROOF: By $\langle 3\rangle 1$ and Theorem 7 in [RRS07] (note that the proof of Theorem 7 in [RRS07] applies for all interaction obligations).
  $\langle 2\rangle 2.$ $Q_3 \subseteq Q_1$
    $\langle 3\rangle 1.$ $Q_3 \subseteq Q_2 \wedge Q_2 \subseteq Q_1$
      PROOF: By assumption $\langle 1\rangle 1$
    $\langle 3\rangle 2.$ Q.E.D.
      PROOF: By $\langle 3\rangle 1$ and transitivity of $\subseteq$
  $\langle 2\rangle 3.$ Q.E.D.
    PROOF: By $\langle 2\rangle 1$ and $\langle 2\rangle 2$
$\langle 1\rangle 2.$ Q.E.D.
  PROOF: $\Rightarrow$-rule

□

**Lemma 16.** *Let $I$ be a system, $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^p$ and let $\oplus\langle I\rangle_{d_1} = (p_1, n_1)$ and $\oplus\langle I\rangle_{d_2} = (p_2, n_2)$. Then $\mathcal{H}^{ll(d_1)} \subseteq \mathcal{H}^{ll(d_2)}$ implies*

*1.* $p_1 \subseteq p_2$
*2.* $n_1 \subseteq n_2$
*3.* $(p_2 \setminus p_1) \cup (n_2 \setminus n_1) \subseteq \mathcal{H}^{ll(d_2)} \setminus \mathcal{H}^{ll(d_1)}$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $\mathcal{H}^{ll(d_1)} \subseteq \mathcal{H}^{ll(d_2)}$
  PROVE: $p_1 \subseteq p_2 \wedge n_1 \subseteq n_2 \wedge (p_2 \setminus p_1) \cup (n_2 \setminus n_1) \subseteq \mathcal{H}^{ll(d_2)} \setminus \mathcal{H}^{ll(d_1)}$
  $\langle 2\rangle 1.$ LET: $m$ be a bijective mapping from $\langle I\rangle_{d_1}$ to $\langle I\rangle_{d_2}$ such that $\forall po \in \langle I\rangle_{d_1} : \pi_1.(\pi_1.po) = \pi_1.(\pi_1.m(po)) \wedge \pi_2.(\pi_1.po) = \pi_2.(\pi_1.m(po)) \cap \mathcal{H}^{ll(d_1)}$

Proof: By assumption $\langle 1\rangle 1$ and definition 30

$\langle 2\rangle 2.$ $(p_2 \setminus p_1) \cup (n_2 \setminus n_1) \subseteq \mathcal{H}^{ll(d_2)} \setminus \mathcal{H}^{ll(d_1)}$

$\langle 3\rangle 1.$ Assume: $t \in (p_2 \setminus p_1) \cup (n_2 \setminus n_1)$
Prove: $t \in \mathcal{H}^{ll(d_2)} \setminus \mathcal{H}^{ll(d_1)}$

$\langle 4\rangle 1.$ Case: $t \in p_2 \setminus p_1$

$\langle 5\rangle 1.$ Let: $po_2' \in \langle I\rangle_{d_2}$ such that $t \in p_2'$
Proof: By assumption $\langle 4\rangle 1$

$\langle 5\rangle 2.$ Let: $po_1' \in \langle I\rangle_{d_1}$ such that $m(po_1') = po_2'$
Proof: By $\langle 2\rangle 1$

$\langle 5\rangle 3.$ $t \in p_1'$
Proof: By $\langle 5\rangle 2$ and $\langle 2\rangle 1$

$\langle 5\rangle 4.$ $\exists po \in \langle I\rangle_{d_1} : t \notin p \cup n$
Proof: By $\langle 5\rangle 3$ and assumption $\langle 4\rangle 1$

$\langle 5\rangle 5.$ $t \notin \mathcal{H}^{ll(d_1)}$
Proof: By $\langle 5\rangle 4$ and definition 30

$\langle 5\rangle 6.$ $t \in \mathcal{H}^{ll(d_2)}$

$\langle 6\rangle 1.$ Assume: $t \notin \mathcal{H}^{ll(d_2)}$
Prove: $\perp$

$\langle 7\rangle 1.$ $\forall po \in \langle I\rangle_{d_2} : t \notin n$
Proof: By assumption $\langle 6\rangle 1$ and definition 30

$\langle 7\rangle 2.$ $\forall po \in \langle I\rangle_{d_2} : t \in p$
Proof: By $\langle 7\rangle 1$ and assumption $\langle 4\rangle 1$ $(t \in p_2)$

$\langle 7\rangle 3.$ $\forall po \in \langle I\rangle_{d_1} : t \in p$
Proof: By $\langle 7\rangle 2$ and $\langle 2\rangle 1$

$\langle 7\rangle 4.$ $: t \in p_1$
Proof: By $\langle 7\rangle 3$

$\langle 7\rangle 5.$ Q.E.D.
Proof: By $\langle 7\rangle 4$ and assumption $\langle 4\rangle 1$

$\langle 6\rangle 2.$ Q.E.D.
Proof: $\perp$-rule

$\langle 5\rangle 7.$ Q.E.D.
Proof: By $\langle 5\rangle 5$ and $\langle 5\rangle 6$

$\langle 4\rangle 2.$ Case: $t \in n_2 \setminus n_1$

$\langle 5\rangle 1.$ $\forall po \in \langle I\rangle_{d_2} : t \in n$
Proof: By assumption $\langle 4\rangle 2$ $(t \in n_2)$

$\langle 5\rangle 2.$ $t \in \mathcal{H}^{ll(d_2)}$
Proof: By $\langle 5\rangle 1$ and definition 30

$\langle 5\rangle 3.$ $t \notin \mathcal{H}^{ll(d_1)}$

$\langle 6\rangle 1.$ Assume: $t \in \mathcal{H}^{ll(d_1)}$
Prove: $\perp$

$\langle 7\rangle 1.$ $\forall po \in \langle I\rangle_{d_1} : t \in p \cup n$
Proof: By assumption $\langle 6\rangle 1$ and definition 30

$\langle 7\rangle 2.$ $t \in p_1 \cup n_1$
Proof: By $\langle 7\rangle 1$

$\langle 7\rangle 3.$ $\forall po \in \langle I\rangle_{d_2} : t \notin p$

Proof: By $\langle 5\rangle 1$ and definition 30

$\langle 7\rangle 4.$ $\forall po \in \langle I\rangle_{d_1} : t \notin p$

Proof: By $\langle 7\rangle 3$ and $\langle 2\rangle 1$ (only the negative sets are different between $\langle I\rangle_{d_1}$ and $\langle I\rangle_{d_2}$)

$\langle 7\rangle 5.$ $t \notin p_1$

Proof: By $\langle 7\rangle 4$

$\langle 7\rangle 6.$ $t \in n_1$

Proof: By $\langle 7\rangle 5$ and $\langle 7\rangle 2$

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

Proof: By $\langle 7\rangle 6$ and assumption $\langle 4\rangle 2$

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

Proof: $\perp$-rule

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

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 3$

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

Proof: By assumption $\langle 3\rangle 1$ the cases $\langle 4\rangle 1$ and $\langle 4\rangle 2$ are exhaustive

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

Proof: $\subseteq$-rule

$\langle 2\rangle 3.$ $n_1 \subseteq n_2$

$\langle 3\rangle 1.$ Assume: $t \in n_1$
Prove: $t \in n_2$

$\langle 4\rangle 1.$ Assume: $t \notin n_2$
Prove: $\perp$

$\langle 5\rangle 1.$ Let: $po'_2 \in \langle I\rangle_{d_2}$ such that $t \notin n'_2$

Proof: By assumption $\langle 4\rangle 1$

$\langle 5\rangle 2.$ Let: $po'_1 \in \langle I\rangle_{d_1}$ such that $m(po'_1) = po'_2$

Proof: By $\langle 2\rangle 1$

$\langle 5\rangle 3.$ $n'_1 = n'_2 \cap \mathcal{H}^{ll(d_1)}$

Proof: By $\langle 5\rangle 2$ and $\langle 2\rangle 1$

$\langle 5\rangle 4.$ $t \notin n'_1$

Proof: By $\langle 5\rangle 3$ and $\langle 5\rangle 1$

$\langle 5\rangle 5.$ $t \notin n_1$

Proof: By $\langle 5\rangle 4$ and $\langle 5\rangle 2$ ($po'_1 \in \langle I\rangle_{d_1}$)

$\langle 5\rangle 6.$ Q.E.D.

Proof: By $\langle 5\rangle 5$ and assumption $\langle 3\rangle 1$

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

Proof: $\perp$-rule

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

Proof: $\subseteq$-rule

$\langle 2\rangle 4.$ $p_1 \subseteq p_2$

$\langle 3\rangle 1.$ Assume: $t \in p_1$
Prove: $t \in p_2$

$\langle 4\rangle 1.$ Assume: $t \notin p_2$
Prove: $\perp$

$\langle 5\rangle 1.$ Let: $po'_1 \in \langle I\rangle_{d_1}$ such that $t \in p'_1$

PROOF: By assumption ⟨3⟩1

⟨5⟩2. LET: $po'_2 \in \langle I \rangle_{d_2}$ such that $m(po'_1) = po'_2$

PROOF: By ⟨2⟩1

⟨5⟩3. $t \in p'_2$

PROOF: By ⟨5⟩1, ⟨5⟩2 and ⟨2⟩1

⟨5⟩4. LET: $po''_2 \in \langle I \rangle_{d_2}$ such that $t \notin p''_2 \cup n''_2$

PROOF: By ⟨5⟩3 (there is a p-obligation in $\langle I \rangle_{d_2}$ where $t$ is positive) and assumption ⟨4⟩1

⟨5⟩5. LET: $po''_1 \in \langle I \rangle_{d_1}$ such that $m(po''_1) = po''_2$

PROOF: By ⟨2⟩1

⟨5⟩6. $t \notin p''_1 \cup n''_1$

PROOF: By ⟨5⟩5, ⟨5⟩4 and ⟨2⟩1

⟨5⟩7. $t \notin p_1$

PROOF: By ⟨5⟩6 and ⟨5⟩5

⟨5⟩8. Q.E.D.

PROOF: By ⟨5⟩7 and assumption ⟨3⟩1

⟨4⟩2. Q.E.D.

PROOF: ⊥-rule

⟨3⟩2. Q.E.D.

PROOF: ⊆-rule

⟨2⟩5. Q.E.D.

PROOF: By ⟨2⟩2, ⟨2⟩3 and ⟨2⟩4

⟨1⟩2. Q.E.D.

PROOF: ⇒-rule

□

**Lemma 17.** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{pl} \langle I \rangle_{d_2} \Rightarrow \oplus\llbracket\ d_1\ \rrbracket \mapsto_r \oplus\langle I \rangle_{d_1}$$

PROOF.

⟨1⟩1. ASSUME: $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{pl} \langle I \rangle_{d_2}$

PROVE: $\oplus\llbracket\ d_1\ \rrbracket \mapsto_r \oplus\langle I \rangle_{d_1}$

⟨2⟩1. $\oplus\llbracket\ d_1\ \rrbracket \rightsquigarrow_r \oplus\llbracket\ d_2\ \rrbracket$

PROOF: By assumption ⟨1⟩1 and Lemma 1

⟨2⟩2. $\oplus\llbracket\ d_2\ \rrbracket \mapsto_r \oplus\langle I \rangle_{d_2}$

PROOF: By assumption ⟨1⟩1, Lemma 1 and definition 32

⟨2⟩3. $\oplus\llbracket\ d_1\ \rrbracket \mapsto_r \oplus\langle I \rangle_{d_2}$

PROOF: By ⟨2⟩1, ⟨2⟩2 and transitivity of $\mapsto_r / \rightsquigarrow_r$ (these are the same)

⟨2⟩4. $\mathcal{H}^{ll(d_1)} \subseteq \mathcal{H}^{ll(d_2)}$

PROOF: By assumption ⟨1⟩1

⟨2⟩5. LET: $\oplus\llbracket\ d_1\ \rrbracket = (p_1, n_1)$

$\oplus\ \langle I \rangle_{d_1} = (p'_1, n'_1)$

$\oplus\ \langle I \rangle_{d_2} = (p'_2, n'_2)$

⟨2⟩6. $p_1 \subseteq p'_2 \cup n'_2 \wedge n_1 \subseteq n'_2$

PROOF: By ⟨2⟩3

$\langle 2\rangle 7.$ $p_1 \cup n_1 \subseteq \mathcal{H}^{ll(d_1)}$

Proof: By $\langle 2\rangle 5$

$\langle 2\rangle 8.$ $(p_2' \setminus p_1') \cup (n_2' \setminus n_1') \subseteq \mathcal{H}^{ll(d_2)} \setminus \mathcal{H}^{ll(d_1)}$

Proof: By $\langle 2\rangle 5$ and Lemma 16

$\langle 2\rangle 9.$ $p_1 \subseteq p_1' \cup n_1' \wedge n_1 \subseteq n_1'$

Proof: By $\langle 2\rangle 6$, $\langle 2\rangle 7$ and $\langle 2\rangle 8$

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

Proof: By $\langle 2\rangle 9$

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

Proof: $\Rightarrow$-rule

□

**Lemma 18.** *Let $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\begin{aligned} po_1 \rightsquigarrow_{pr} \bar{\oplus}[\![\, d_1 \,]\!] \wedge po_2 \rightsquigarrow_{pr} \bar{\oplus}[\![\, d_2 \,]\!] \Rightarrow\ & \pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{seq}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \succsim po_2)\ \wedge \\ & \pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{par}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \parallel po_2)\ \wedge \\ & \pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{alt}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \uplus po_2) \end{aligned}$$

Proof.

$\langle 1\rangle 1.$ Assume: $po_1 \rightsquigarrow_{pr} \bar{\oplus}[\![\, d_1 \,]\!] \wedge po_2 \rightsquigarrow_{pr} \bar{\oplus}[\![\, d_2 \,]\!]$

Prove: $\pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{seq}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \succsim po_2) \wedge$
$\pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{par}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \parallel po_2) \wedge$
$\pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{alt}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \uplus po_2)$

$\langle 2\rangle 1.$ $\pi_2.(\bar{\oplus}([\![\, d_1 \ \mathsf{seq}\ d_2 \,]\!])) \subseteq \pi_2.(po_1 \succsim po_2)$

$\langle 3\rangle 1.$ $\pi_2.\bar{\oplus}([\![\, d_1 \ \mathsf{seq}\ d_2 \,]\!]) \subseteq \{1\}$

Proof: By Lemma 2

$\langle 3\rangle 2.$ $1 \in \pi_2.\bar{\oplus}([\![\, d_1 \ \mathsf{seq}\ d_2 \,]\!]) \Rightarrow 1 \in \pi_2.(po_1 \succsim po_2)$

$\langle 4\rangle 1.$ Assume: $1 \in \pi_2.\bar{\oplus}([\![\, d_1 \ \mathsf{seq}\ d_2 \,]\!])$

Prove: $1 \in \pi_2.(po_1 \succsim po_2)$

$\langle 5\rangle 1.$ Assume: $1 \notin \pi_2.(po_1 \succsim po_2)$

Prove: $\bot$

$\langle 6\rangle 1.$ $1 \notin \pi_2.po_1 \vee 1 \notin \pi_2.po_2$

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

$\langle 6\rangle 2.$ Case: $1 \notin \pi_2.po_1$

$\langle 7\rangle 1.$ $1 \notin \pi_2.\bar{\oplus}[\![\, d_1 \,]\!]$

Proof: By assumption $\langle 6\rangle 2$ and assumption $\langle 1\rangle 1$

$\langle 7\rangle 2.$ $\pi_2.\bar{\oplus}[\![\, d_1 \,]\!] = \emptyset$

Proof: By $\langle 7\rangle 1$ and Lemma 2

$\langle 7\rangle 3.$ $\exists po \in [\![\, d_1 \,]\!] : \pi_2.po = \emptyset$

Proof: By $\langle 7\rangle 2$

$\langle 7\rangle 4.$ $\exists po \in [\![\, d_1 \,]\!] \succsim [\![\, d_2 \,]\!] : \pi_2.po = \emptyset$

Proof: By $\langle 7\rangle 3$

$\langle 7\rangle 5.$ $\pi_2.\bar{\oplus}([\![\, d_1 \,]\!] \succsim [\![\, d_2 \,]\!]) = \emptyset$

Proof: By $\langle 7\rangle 4$ and definitions 6 and 7

$\langle 7\rangle 6.$ Q.E.D.

PROOF: By $\langle 7\rangle 5$ and assumption $\langle 4\rangle 1$

$\langle 6\rangle 3$. CASE: $1 \notin \pi_2.po_2$

PROOF: Similar to $\langle 6\rangle 2$

$\langle 6\rangle 4$. Q.E.D.

PROOF: By $\langle 6\rangle 1$, the cases $\langle 6\rangle 2$ and $\langle 6\rangle 3$ are exhaustive

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

PROOF: $\perp$-rule

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

PROOF: $\Rightarrow$-rule

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

PROOF: By $\langle 3\rangle 1$ and $\langle 3\rangle 2$

$\langle 2\rangle 2$. $\pi_2.(\bar{\oplus}(\llbracket\ d_1 \ \mathsf{par}\ d_2 \ \rrbracket)) \subseteq \pi_2.(po_1 \parallel po_2)$

PROOF: Similar to $\langle 2\rangle 1$; just replace seq with par and $\succsim$ with $\|$.

$\langle 2\rangle 3$. $\pi_2.(\bar{\oplus}(\llbracket\ d_1 \ \mathsf{alt}\ d_2 \ \rrbracket)) \subseteq \pi_2.(po_1 \uplus po_2)$

PROOF: Similar to $\langle 2\rangle 1$; just replace seq with alt and $\succsim$ with $\uplus$.

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

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$ and $\langle 2\rangle 3$

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

PROOF: $\Rightarrow$-rule

□

**Lemma 19.** *Let $O_1$, $O_2$, $O_1'$ and $O_2'$ be sets of p-obligations. Then*

$$O_1 \leadsto_{pl} O_1' \wedge O_2 \leadsto_{pl} O_2' \Rightarrow \oplus(O_1 \uplus O_2) \leadsto_r \oplus(O_1' \uplus O_2')$$

PROOF.

$\langle 1\rangle 1$. ASSUME: $O_1 \leadsto_{pl} O_1' \wedge O_2 \leadsto_{pl} O_2'$
PROVE: $\oplus(O_1 \uplus O_2) \leadsto_r \oplus(O_1' \uplus O_2')$

$\langle 2\rangle 1$. $\oplus O_1 \leadsto_r \oplus O_1' \wedge \oplus O_2 \leadsto_r \oplus O_2'$

PROOF: By assumption $\langle 1\rangle 1$ and Lemma 1

$\langle 2\rangle 2$. LET: $(p_3, n_3) = \oplus(O_1 \uplus O_2)$
$(p_4, n_4) = \oplus(O_1' \uplus O_2')$

$\langle 2\rangle 3$. $n_3 \subseteq n_4$

$\langle 3\rangle 1$. ASSUME: $t \in n_3$
PROVE: $t \in n_4$

$\langle 4\rangle 1$. $\forall po \in O_1 \uplus O_2 : t \in n$

PROOF: By assumption $\langle 3\rangle 1$

$\langle 4\rangle 2$. $(\forall po \in O_1 : t \in n) \vee (\forall po \in O_2 : t \in n)$

$\langle 5\rangle 1$. ASSUME: $(\exists po \in O_1 : t \notin n) \wedge (\exists po \in O_2 : t \notin n)$
PROVE: $\perp$

$\langle 6\rangle 1$. LET: $po_1 \in O_1$ s.t. $t \notin n_1$
$po_2 \in O_2$ s.t. $t \notin n_2$

PROOF: By assumption $\langle 5\rangle 1$

$\langle 6\rangle 2$. $t \notin n_1 \cup n_2$

PROOF: By $\langle 6\rangle 1$

$\langle 6\rangle 3$. $\exists po \in O_1 \uplus O_2 : t \notin n$

Proof: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$

$\langle 6\rangle 4$. Q.E.D.

Proof: By $\langle 6\rangle 3$ and $\langle 4\rangle 1$

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

Proof: $\bot$-rule

$\langle 4\rangle 3$. Case: $\forall po_1 \in O_1 : t \in n_1$

$\langle 5\rangle 1$. $t \in \pi_2. \oplus O_1$

Proof: By assumption $\langle 4\rangle 3$ and definition 4

$\langle 5\rangle 2$. $t \in \pi_2. \oplus O_1'$

Proof: By $\langle 5\rangle 1$ and $\langle 2\rangle 1$

$\langle 5\rangle 3$. $\forall po \in O_1' : t \in n$

Proof: By $\langle 5\rangle 2$

$\langle 5\rangle 4$. $\forall po \in O_1' \uplus O_2' : t \in n$

Proof: By $\langle 5\rangle 3$ and definition 47

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

Proof: By $\langle 5\rangle 4$ and definition 4

$\langle 4\rangle 4$. Case: $\forall po_2 \in O_2 : t \in n_2$

Proof: Similar to case $\langle 4\rangle 3$

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

Proof: By $\langle 4\rangle 2$ the cases $\langle 4\rangle 3$ and $\langle 4\rangle 4$ are exhaustive

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

Proof: $\subseteq$-rule

$\langle 2\rangle 4$. $p_3 \subseteq p_4 \cup n_4$

$\langle 3\rangle 1$. Assume: $t \in p_3$

Prove: $t \in p_4 \cup n_4$

$\langle 4\rangle 1$. Assume: $t \notin p_4 \cup n_4$

Prove: $\bot$

$\langle 5\rangle 1$. $\exists po \in O_1' \uplus O_2' : t \notin p \cup n$

Proof: By assumption $\langle 4\rangle 1$

$\langle 5\rangle 2$. Let: $po_1' \in O_1', po_2' \in O_2'$ s.t. $t \notin p_1' \cup n_1' \cup p_2' \cup n_2'$

Proof: By $\langle 5\rangle 1$

$\langle 5\rangle 3$. Let: $po_1'' \in O_1, S_1 \subseteq O_1'$ s.t. $po_1' \in S_1 \wedge po_1'' \rightsquigarrow_{pr} \bar{\oplus} S_1$

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

$\langle 5\rangle 4$. $t \notin \pi_1. \oplus S_1 \cup \pi_2. \oplus S_1$

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 3$

$\langle 5\rangle 5$. $t \notin p_1'' \cup n_1''$

Proof: By $\langle 5\rangle 3$ and $\langle 5\rangle 4$

$\langle 5\rangle 6$. Let: $po_2'' \in O_2, S_2 \subseteq O_2'$ s.t. $po_2' \in S_2 \wedge po_2'' \rightsquigarrow_{pr} \bar{\oplus} S_2$

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

$\langle 5\rangle 7$. $t \notin \pi_1. \oplus S_2 \cup \pi_2. \oplus S_2$

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 6$

$\langle 5\rangle 8$. $t \notin p_2'' \cup n_2''$

Proof: By $\langle 5\rangle 6$ and $\langle 5\rangle 7$

$\langle 5\rangle 9$. $t \notin p_1'' \cup n_1'' \cup p_2'' \cup n_2''$

Proof: By $\langle 5\rangle 5$ and $\langle 5\rangle 8$

$\langle 5\rangle$10. $\exists po \in O_1 \uplus O_2 : t \notin p \cup n$
PROOF: By $\langle 5\rangle$9
$\langle 5\rangle$11. $t \notin p_3 \cup n_3$
PROOF: By $\langle 5\rangle$10
$\langle 5\rangle$12. Q.E.D.
PROOF: By assumption $\langle 3\rangle$1 and $\langle 5\rangle$11
$\langle 4\rangle$2. Q.E.D.
PROOF: $\perp$-rule
$\langle 3\rangle$2. Q.E.D.
PROOF: $\subseteq$-rule
$\langle 2\rangle$5. Q.E.D.
PROOF: By $\langle 2\rangle$3 and $\langle 2\rangle$4
$\langle 1\rangle$2. Q.E.D.
PROOF: $\Rightarrow$-rule

□

**Lemma 20.** *Let $O_i$ and $O'_i$ be sets of p-obligations. Then*

$$(\forall i \leq n : \oplus O_i \rightsquigarrow_{nr} \oplus O'_i) \Rightarrow \oplus \bigcup_{i=1}^{n} O_i \rightsquigarrow_{nr} \oplus \bigcup_{i=1}^{n} O'$$

PROOF.

$\langle 1\rangle$1. ASSUME: $\forall i \leq n : \oplus O_i \rightsquigarrow_{nr} \oplus O'_i$
PROVE: $\oplus \bigcup_{i=1}^{n} O_i \rightsquigarrow_{nr} \oplus \bigcup_{i=1}^{n} O'$
$\langle 2\rangle$1. LET: $(p, n) = \oplus \bigcup_{i=1}^{n} O_i$
$(p', n') = \oplus \bigcup_{i=1}^{n} O'_i$
$(p_i, n_i) = \oplus O_i$ for each $i \leq n$
$(p'_i, n'_i) = \oplus O'_i$ for each $i \leq n$
$\langle 2\rangle$2. $(p, n) \rightsquigarrow_r (p', n')$
PROOF: By assumption $\langle 1\rangle$1 and Lemma 10
$\langle 2\rangle$3. $p \cup n = p' \cup n'$
$\langle 3\rangle$1. $\forall i \leq n : p_i \cup n_i = p'_i \cup n'_i$
PROOF: By assumption $\langle 1\rangle$1
$\langle 3\rangle$2. Q.E.D.
PROOF: By $\langle 3\rangle$1 and definition 4
$\langle 2\rangle$4. Q.E.D.
PROOF: By $\langle 2\rangle$2 and $\langle 2\rangle$3
$\langle 1\rangle$2. Q.E.D.
PROOF: $\Rightarrow$-rule

□

**Lemma 21.** *Let $d = \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)$ and $d' = \mathsf{palt}(d'_1;Q'_1, \ldots, d'_n;Q'_n)$, where $d_1, \ldots d_n, d'_1, \ldots, d'_n$ are sequence diagrams in $\mathcal{D}^p$. Then*

$$(\forall i \leq n : [\![\ d_i\ ]\!] \rightsquigarrow_{pg} [\![\ d'_i\ ]\!] \wedge Q'_i \subseteq Q_i) \Rightarrow \pi_2.\bar{\oplus}[\![\ d'\ ]\!] \subseteq \pi_2.\bar{\oplus}[\![\ d\ ]\!]$$

Proof.

$\langle 1 \rangle 1.$ Assume: $\forall i \leq n : [\![ \ d_i \ ]\!] \rightsquigarrow_{pg} [\![ \ d'_i \ ]\!] \wedge Q'_i \subseteq Q_i$
 Prove: $\pi_2.\bar{\bigoplus}[\![ \ d' \ ]\!] \subseteq \pi_2.\bar{\bigoplus}[\![ \ d \ ]\!]$

$\langle 2 \rangle 1.$ $1 \in \pi_2.\bar{\bigoplus}[\![ \ d' \ ]\!] \Rightarrow 1 \in \pi_2.\bar{\bigoplus}[\![ \ d \ ]\!]$

$\langle 3 \rangle 1.$ Assume: $1 \in \pi_2.\bar{\bigoplus}[\![ \ d' \ ]\!]$
 Prove: $1 \in \pi_2.\bar{\bigoplus}[\![ \ d \ ]\!]$

$\langle 4 \rangle 1.$ $\forall po \in [\![ \ d' \ ]\!] : \pi_2.po \neq \emptyset$
Proof: By assumption $\langle 3 \rangle 1$

$\langle 4 \rangle 2.$ $\forall i \leq n, po \in [\![ \ d'_i \ ]\!] : \pi_2.po \neq \emptyset$
Proof: By $\langle 4 \rangle 1$

$\langle 4 \rangle 3.$ $\forall i \leq n, po \in [\![ \ d_i \ ]\!] : \pi_2.po \neq \emptyset$
Proof: By $\langle 4 \rangle 2$ and assumption $\langle 1 \rangle 1$ (since each p-obligation in every $[\![ \ d_i \ ]\!]$ must be represented in $[\![ \ d'_i \ ]\!]$)

$\langle 4 \rangle 4.$ $\forall i \leq n : Q'_i \neq \emptyset$
Proof: By assumption $\langle 3 \rangle 1$

$\langle 4 \rangle 5.$ $\forall i \leq n : Q_i \neq \emptyset$
Proof: By $\langle 4 \rangle 4$ and assumption $\langle 1 \rangle 1$

$\langle 4 \rangle 6.$ $\forall po \in [\![ \ d \ ]\!] : \pi_2.po \neq \emptyset$
Proof: By $\langle 4 \rangle 3$ and $\langle 4 \rangle 5$

$\langle 4 \rangle 7.$ $\pi_2.\bar{\bigoplus}[\![ \ d \ ]\!] \neq \emptyset$
Proof: By $\langle 4 \rangle 6$

$\langle 4 \rangle 8.$ Q.E.D.
Proof: By $\langle 4 \rangle 7$ and Lemma 2

$\langle 3 \rangle 2.$ Q.E.D.
Proof: $\Rightarrow$-rule

$\langle 2 \rangle 2.$ Q.E.D.
Proof: By $\langle 2 \rangle 1$ and Lemma 2

$\langle 1 \rangle 2.$ Q.E.D.
Proof: $\Rightarrow$-rule

□

**Lemma 22.** *Let $d_1$, $d_2$, $d'_1$ and $d'_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![ \ d_1 \ ]\!] \rightsquigarrow_{pnl} [\![ \ d'_1 \ ]\!] \wedge [\![ \ d_2 \ ]\!] \rightsquigarrow_{pnl} [\![ \ d'_2 \ ]\!] \Rightarrow trs(\bar{\bigoplus}[\![ \ d_1 \ \mathsf{seq} \ d_2 \ ]\!]) = trs(\bar{\bigoplus}[\![ \ d'_1 \ \mathsf{seq} \ d'_2 \ ]\!])$$

Proof.

$\langle 1 \rangle 1.$ Assume: $[\![ \ d_1 \ ]\!] \rightsquigarrow_{pnl} [\![ \ d'_1 \ ]\!] \wedge [\![ \ d_2 \ ]\!] \rightsquigarrow_{pnl} [\![ \ d'_2 \ ]\!]$
 Prove: $trs(\bar{\bigoplus}[\![ \ d_1 \ \mathsf{seq} \ d_2 \ ]\!]) = trs(\bar{\bigoplus}[\![ \ d'_1 \ \mathsf{seq} \ d'_2 \ ]\!])$

$\langle 2 \rangle 1.$ $trs(\bar{\bigoplus}[\![ \ d_1 \ \mathsf{seq} \ d_2 \ ]\!]) \subseteq trs(\bar{\bigoplus}[\![ \ d'_1 \ \mathsf{seq} \ d'_2 \ ]\!])$

$\langle 3 \rangle 1.$ Assume: $t \in trs(\bar{\bigoplus}[\![ \ d_1 \ \mathsf{seq} \ d_2 \ ]\!])$
 Prove: $t \in trs(\bar{\bigoplus}[\![ \ d'_1 \ \mathsf{seq} \ d'_2 \ ]\!])$

$\langle 4 \rangle 1.$ Assume: $t \notin trs(\bar{\bigoplus}[\![ \ d'_1 \ \mathsf{seq} \ d'_2 \ ]\!])$
 Prove: $\perp$

$\langle 5 \rangle 1.$ Let: $po' \in [\![ \ d'_1 \ \mathsf{seq} \ d'_2 \ ]\!]$ such that $t \notin trs(po')$
Proof: By assumption $\langle 4 \rangle 1$

⟨5⟩2. Let: $po'_1 \in \llbracket\ d'_1\ \rrbracket$ and $po'_2 \in \llbracket\ d'_2\ \rrbracket$ such that $po' = po'_1 \succsim po'_2$

Proof: By ⟨5⟩1

⟨5⟩3. Let: $po_1 \in \llbracket\ d_1\ \rrbracket, S_1 \subseteq \llbracket\ d'_1\ \rrbracket$ such that $po'_1 \in S_1 \wedge po_1 \rightsquigarrow_{pnr} \bar{\oplus} S_1$
$po_2 \in \llbracket\ d_2\ \rrbracket, S_2 \subseteq \llbracket\ d'_2\ \rrbracket$ such that $po'_2 \in S_2 \wedge po_2 \rightsquigarrow_{pnr} \bar{\oplus} S_2$

Proof: By ⟨5⟩2 and assumption ⟨1⟩1

⟨5⟩4. $t \notin trs(po'_1 \succsim po'_2)$

Proof: By ⟨5⟩1 and ⟨5⟩2

⟨5⟩5. $t \notin trs(\bar{\oplus}(S_1 \succsim S_2))$

⟨6⟩1. $po'_1 \succsim po'_2 \in S_1 \succsim S_2$

Proof: By ⟨5⟩3

⟨6⟩2. Q.E.D.

Proof: By ⟨6⟩1 and ⟨5⟩4

⟨5⟩6. $t \notin trs(\bar{\oplus} S_1 \succsim \bar{\oplus} S_2)$

⟨6⟩1. $\bar{\oplus} S_1 \succsim \bar{\oplus} S_2 \rightsquigarrow_r \bar{\oplus}(S_1 \succsim S_2)$

Proof: By Lemma 4

⟨6⟩2. $trs(\bar{\oplus} S_1 \succsim \bar{\oplus} S_2) \subseteq trs(\bar{\oplus}(S_1 \succsim S_2))$

Proof: By ⟨6⟩1

⟨6⟩3. Q.E.D.

Proof: By ⟨6⟩2 and ⟨5⟩5

⟨5⟩7. $t \notin trs(po_1 \succsim po_2)$

⟨6⟩1. $trs(po_1) = trs(\bar{\oplus} S_1) \wedge trs(po_2) = trs(\bar{\oplus} S_2)$

Proof: By ⟨5⟩3

⟨6⟩2. $trs(po_1 \succsim po_2) = trs(\bar{\oplus} S_1 \succsim \bar{\oplus} S_2)$

Proof: By ⟨6⟩1

⟨6⟩3. Q.E.D.

Proof: By ⟨6⟩2 and ⟨5⟩6

⟨5⟩8. $po_1 \succsim po_2 \in \llbracket\ d_1 \ \mathsf{seq}\ d_2\ \rrbracket$

Proof: By ⟨5⟩3

⟨5⟩9. $t \notin trs(\bar{\oplus}\llbracket\ d_1 \ \mathsf{seq}\ d_2\ \rrbracket)$

Proof: By ⟨5⟩7 and ⟨5⟩8

⟨5⟩10. Q.E.D.

Proof: By assumption ⟨3⟩1 and ⟨5⟩9

⟨4⟩2. Q.E.D.

Proof: $\bot$-rule

⟨3⟩2. Q.E.D.

Proof: $\subseteq$-rule

⟨2⟩2. $trs(\bar{\oplus}\llbracket\ d'_1 \ \mathsf{seq}\ d'_2\ \rrbracket) \subseteq trs(\bar{\oplus}\llbracket\ d_1 \ \mathsf{seq}\ d_2\ \rrbracket)$

⟨3⟩1. Assume: $t \in trs(\bar{\oplus}\llbracket\ d'_1 \ \mathsf{seq}\ d'_2\ \rrbracket)$
Prove: $t \in trs(\bar{\oplus}\llbracket\ d_1 \ \mathsf{seq}\ d_2\ \rrbracket)$

⟨4⟩1. Let: $po'_1 \in \llbracket\ d'_1\ \rrbracket$ s.t. $po'_1 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d'_1\ \rrbracket \wedge Q'_1 \subseteq \{1\}$

Proof: By Lemma 12

⟨4⟩2. Let: $po'_2 \in \llbracket\ d'_2\ \rrbracket$ s.t. $po'_2 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d'_2\ \rrbracket \wedge Q'_2 \subseteq \{1\}$

Proof: By Lemma 12

⟨4⟩3. $t \in trs(po'_1 \succsim po'_2)$

⟨5⟩1. $po'_1 \succsim po'_2 \in \llbracket\ d'_1 \ \mathsf{seq}\ d'_2\ \rrbracket$

Proof: By ⟨4⟩1 and ⟨4⟩2

⟨5⟩2. $\forall po \in [\![\, d'_1 \text{ seq } d'_2 \,]\!] : t \in p \cup n$

Proof: By assumption ⟨3⟩1

⟨5⟩3. Q.E.D.

Proof: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩4. $\forall po \in [\![\, d_1 \text{ seq } d_2 \,]\!] : t \in p \cup n$

⟨5⟩1. Assume: $po'' \in [\![\, d_1 \text{ seq } d_2 \,]\!]$
Prove: $t \in p'' \cup n''$

⟨6⟩1. Let: $t_1 \in p'_1 \cup n'_1, t_2 \in p'_2 \cup n'_2$ s.t. $t \in \{t_1\} \succsim \{t_2\}$

Proof: By ⟨4⟩3

⟨6⟩2. Let: $po''_1 \in [\![\, d_1 \,]\!], po''_2 \in [\![\, d_2 \,]\!]$ s.t. $po'' = po''_1 \succsim po''_2$

Proof: By assumption ⟨5⟩1

⟨6⟩3. $t_1 \in p''_1 \cup n''_1$

⟨7⟩1. Assume: $t_1 \notin p''_1 \cup n''_1$
Prove: $\perp$

⟨8⟩1. $\forall po \in [\![\, d'_1 \,]\!] : t_1 \in p \cup n$

⟨9⟩1. $t_1 \in trs(\bar{\oplus}[\![\, d'_1 \,]\!])$

Proof: By ⟨6⟩1 and ⟨4⟩1

⟨9⟩2. Q.E.D.

Proof: By ⟨9⟩1

⟨8⟩2. Let: $po_3 \in [\![\, d_1 \,]\!]$ s.t. $po_3 \rightsquigarrow_{pnr} \bar{\oplus}[\![\, d_1 \,]\!] \wedge Q_3 \subseteq \{1\}$

Proof: By Lemma 12

⟨8⟩3. $t_1 \notin p_3 \cup n_3$

⟨9⟩1. $\exists po \in [\![\, d_1 \,]\!] : t_1 \notin p \cup n$

Proof: By assumption ⟨7⟩1 and ⟨6⟩2

⟨9⟩2. $t_1 \notin trs(\bar{\oplus}[\![\, d_1 \,]\!])$

Proof: By ⟨9⟩1

⟨9⟩3. Q.E.D.

Proof: By ⟨9⟩2 and ⟨8⟩2

⟨8⟩4. Let: $po'_3 \in [\![\, d'_1 \,]\!]$ s.t. $po_3 \rightsquigarrow_{pnr} po'_3$

Proof: By ⟨8⟩2 ($po_3 \in [\![\, d_1 \,]\!]$ and $0 \notin Q_3$) and assumption ⟨1⟩1

⟨8⟩5. $t_1 \notin p'_3 \cup n'_3$

Proof: By ⟨8⟩3 and ⟨8⟩4

⟨8⟩6. $t_1 \in p'_3 \cup n'_3$

Proof: By ⟨8⟩1 and ⟨8⟩4

⟨8⟩7. Q.E.D.

Proof: By ⟨8⟩5 and ⟨8⟩6

⟨7⟩2. Q.E.D.

Proof: $\perp$-rule

⟨6⟩4. $t_2 \in p''_2 \cup n''_2$

Proof: Similar to ⟨6⟩3

⟨6⟩5. Q.E.D.

Proof: By ⟨6⟩1, ⟨6⟩2, ⟨6⟩3 and ⟨6⟩4

⟨5⟩2. Q.E.D.

PROOF: $\forall$-rule

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

PROOF: By $\langle 4\rangle 4$

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

PROOF: $\subseteq$-rule

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

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

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

PROOF: $\Rightarrow$-rule

□

**Lemma 23.** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\, d_1 \,\rrbracket \rightsquigarrow_{pnl} \llbracket\, d_1' \,\rrbracket \wedge \llbracket\, d_2 \,\rrbracket \rightsquigarrow_{pnl} \llbracket\, d_2' \,\rrbracket \Rightarrow trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{par}\; d_2 \,\rrbracket) = trs(\bar{\oplus}\llbracket\, d_1' \;\mathsf{par}\; d_2' \,\rrbracket)$$

PROOF. The proof is similar to the proof of Lemma 22; just replace seq with par, $\succsim$ with $\|$ and the reference to Lemma 4 with a reference to Lemma 5 □

**Lemma 24.** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\, d_1 \,\rrbracket \rightsquigarrow_{pnl} \llbracket\, d_1' \,\rrbracket \wedge \llbracket\, d_2 \,\rrbracket \rightsquigarrow_{pnl} \llbracket\, d_2' \,\rrbracket \Rightarrow trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket) = trs(\bar{\oplus}\llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket)$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $\llbracket\, d_1 \,\rrbracket \rightsquigarrow_{pnl} \llbracket\, d_1' \,\rrbracket \wedge \llbracket\, d_2 \,\rrbracket \rightsquigarrow_{pnl} \llbracket\, d_2' \,\rrbracket$

PROVE: $trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket) = trs(\bar{\oplus}\llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket)$

$\langle 2\rangle 1.$ $trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket) \subseteq trs(\bar{\oplus}\llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket)$

$\langle 3\rangle 1.$ $\llbracket\, d_1 \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d_1' \,\rrbracket \wedge \llbracket\, d_2 \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d_2' \,\rrbracket$

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

$\langle 3\rangle 2.$ $\oplus\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket \rightsquigarrow_{r} \oplus\llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket$

PROOF: By $\langle 3\rangle 1$ and Lemma 19

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

PROOF: By $\langle 3\rangle 2$

$\langle 2\rangle 2.$ $trs(\bar{\oplus}\llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket) \subseteq trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket)$

$\langle 3\rangle 1.$ ASSUME: $t \in trs(\bar{\oplus}\llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket)$

PROVE: $t \in trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket)$

$\langle 4\rangle 1.$ ASSUME: $t \notin trs(\bar{\oplus}\llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket)$

PROVE: $\perp$

$\langle 5\rangle 1.$ $\forall po \in \llbracket\, d_1' \;\mathsf{alt}\; d_2' \,\rrbracket : t \in p \cup n$

PROOF: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ $\exists po \in \llbracket\, d_1 \;\mathsf{alt}\; d_2 \,\rrbracket : t \notin p \cup n$

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

$\langle 5\rangle 3.$ $\exists po \in \llbracket\, d_1 \,\rrbracket : t \notin p \cup n \wedge \exists po \in \llbracket\, d_2 \,\rrbracket : t \notin p \cup n$

PROOF: By $\langle 5\rangle 2$

$\langle 5\rangle 4.$ LET: $po_1 \in \llbracket\, d_1 \,\rrbracket$ s.t. $po_1 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\, d_1 \,\rrbracket \wedge Q_1 \subseteq \{1\}$

PROOF: By Lemma 12

$\langle 5\rangle 5.$ LET: $po_1' \in \llbracket\, d_1' \,\rrbracket$ s.t. $po_1 \rightsquigarrow_{pnr} po_1'$

PROOF: By $\langle 5\rangle 4$ and assumption $\langle 1\rangle 1$

$\langle 5\rangle 6$. LET: $po_2 \in \llbracket\ d_2\ \rrbracket$ s.t. $po_2 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_2\ \rrbracket \wedge Q_2 \subseteq \{1\}$

PROOF: By Lemma 12

$\langle 5\rangle 7$. LET: $po_2' \in \llbracket\ d_2'\ \rrbracket$ s.t. $po_2 \rightsquigarrow_{pnr} po_2'$

PROOF: By $\langle 5\rangle 6$ and assumption $\langle 1\rangle 1$

$\langle 5\rangle 8$. $t \notin p_1' \cup n_1'$

$\langle 6\rangle 1$. $t \notin trs(\bar{\oplus}\llbracket\ d_1\ \rrbracket)$

PROOF: By $\langle 5\rangle 3$

$\langle 6\rangle 2$. $t \notin p_1 \cup n_1$

PROOF: By $\langle 6\rangle 1$ and $\langle 5\rangle 4$

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

PROOF: By $\langle 6\rangle 2$ and $\langle 5\rangle 5$

$\langle 5\rangle 9$. $t \notin p_2' \cup n_2'$

$\langle 6\rangle 1$. $t \notin trs(\bar{\oplus}\llbracket\ d_2\ \rrbracket)$

PROOF: By $\langle 5\rangle 3$

$\langle 6\rangle 2$. $t \notin p_2 \cup n_2$

PROOF: By $\langle 6\rangle 1$ and $\langle 5\rangle 6$

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

PROOF: By $\langle 6\rangle 2$ and $\langle 5\rangle 7$

$\langle 5\rangle 10$. $t \notin trs(po_1' \uplus po_2')$

PROOF: By $\langle 5\rangle 8$ and $\langle 5\rangle 9$

$\langle 5\rangle 11$. $po_1' \uplus po_2' \in \llbracket\ d_1'\ \mathsf{alt}\ d_2'\ \rrbracket$

PROOF: By $\langle 5\rangle 5$ and $\langle 5\rangle 7$

$\langle 5\rangle 12$. $\exists po \in \llbracket\ d_1'\ \mathsf{alt}\ d_2'\ \rrbracket : t \notin p \cup n$

PROOF: By $\langle 5\rangle 11$

$\langle 5\rangle 13$. Q.E.D.

PROOF: By $\langle 5\rangle 12$ and $\langle 3\rangle 1$

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

PROOF: $\perp$-rule

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

PROOF: $\subseteq$-rule

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

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

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

PROOF: $\Rightarrow$-rule

□

**Lemma 25.** *Let $O$ be a set of p-obligations. Then*

$$((p, n), Q) \in O \Rightarrow trs(\oplus O) \subseteq p \cup n$$

PROOF.

$\langle 1\rangle 1$. LET: $(p', n') = \oplus O$, i.e. $trs(\oplus O) = p' \cup n'$

$\langle 1\rangle 2$. ASSUME: $((p, n), Q) \in O$

PROVE: $p' \cup n' \subseteq p \cup n$

$\langle 2\rangle 1$. ASSUME: $t \in p' \cup n'$

Prove: $t \in p \cup n$

⟨3⟩1. $\forall((p'', n''), Q'') \in O : t \in p'' \cup n''$

Proof: By assumption ⟨2⟩1, ⟨1⟩1 and definition 4

⟨3⟩2. Q.E.D.

Proof: By assumption ⟨1⟩2 and ⟨3⟩1

⟨2⟩2. Q.E.D.

Proof: $\subseteq$-rule

⟨1⟩3. Q.E.D.

Proof: $\Rightarrow$-rule

□

**Lemma 26 (Transitivity of $\rightsquigarrow_{pnr}$).** *Let $po_1$, $po_2$, and $po_3$ be p-obligations. Then*

$$po_1 \rightsquigarrow_{pnr} po_2 \wedge po_2 \rightsquigarrow_{pnr} po_3 \Rightarrow po_1 \rightsquigarrow_{pnr} po_3$$

Proof.

⟨1⟩1. Assume: $po_1 \rightsquigarrow_{pnr} po_2 \wedge po_2 \rightsquigarrow_{pnr} po_3$

Prove: $po_1 \rightsquigarrow_{pnr} po_3$

⟨2⟩1. $Q_3 \subseteq Q_1$

⟨3⟩1. $Q_2 \subseteq Q_1 \wedge Q_3 \subseteq Q_2$

Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1

⟨2⟩2. $(p_1, n_1) \rightsquigarrow_r (p_3, n_3)$

⟨3⟩1. $(p_1, n_1) \rightsquigarrow_r (p_2, n_2) \wedge (p_2, n_2) \rightsquigarrow_r (p_3, n_3)$

Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1 and Lemma 26 in [HHRS06]

⟨2⟩3. $p_1 \cup n_1 = p_3 \cup n_3$

⟨3⟩1. $p_1 \cup n_1 = p_2 \cup n_2 \wedge p_2 \cup n_2 = p_3 \cup n_3$

Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1

⟨2⟩4. Q.E.D.

Proof: By ⟨2⟩1, ⟨2⟩2 and ⟨2⟩3

⟨1⟩2. Q.E.D.

Proof: $\Rightarrow$-rule

□

**Lemma 27.** *Let $(traces(I), \mathcal{F}_I, f_I)$ be a probability space representing system $I$ as described in Section 5. Then*

$$\forall t \in traces(I) : \{t\} \in \mathcal{F}_I$$

Proof. Note: In this proof we write $c(t)$ instead of $c_t$ for notational reasons.

⟨1⟩1. Assume: $t_1 \in traces(I)$

PROVE: $\{t_1\} \in \mathcal{F}_I$

$\langle 2 \rangle 1.$ CASE: $\#t_1 \in \mathbb{N}_0$ (i.e. $t_1$ is finite)

$\langle 3 \rangle 1.$ $c(t_1) \in \mathcal{F}_I$

$\langle 4 \rangle 1.$ $c(t_1) \in C_I$

PROOF: By assumption $\langle 1 \rangle 1$, assumption $\langle 2 \rangle 1$ and definition 29

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

PROOF: By $\langle 4 \rangle 1$, since $C_I \subseteq \mathcal{F}_I$, which is ensured by the requirement that $\mathcal{F}_I$ is the cone-$\sigma$-field of $traces(I)$

$\langle 3 \rangle 2.$ LET: $S = \{t \in \mathcal{H} \mid \#t = \#t_1 + 1 \wedge \exists t' \in c(t_1) : t \sqsubseteq t'\}$

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

PROOF: By $\langle 3 \rangle 2$ and assumption $\langle 2 \rangle 1$

$\langle 3 \rangle 4.$ CASE: $S = \emptyset$

$\langle 4 \rangle 1.$ $c(t_1) = \{t_1\}$

PROOF: By $\langle 3 \rangle 2$ and assumption $\langle 3 \rangle 4$

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

PROOF: By $\langle 4 \rangle 1$ and $\langle 3 \rangle 1$

$\langle 3 \rangle 5.$ CASE: $S \neq \emptyset$

$\langle 4 \rangle 1.$ $\forall t \in S : c(t) \in \mathcal{F}_I$

$\langle 5 \rangle 1.$ $\forall t \in S : c(t) \in C_I$

PROOF: By $\langle 3 \rangle 3$, $\langle 3 \rangle 2$ and definition 29

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

PROOF: By $\langle 5 \rangle 1$, since $C_I \subseteq \mathcal{F}_I$

$\langle 4 \rangle 2.$ $\bigcup\limits_{t \in S} c(t) \in \mathcal{F}_I$

$\langle 5 \rangle 1.$ $\exists j \in \mathbb{N} : \forall t \in S : \#t = j$

PROOF: By assumption $\langle 2 \rangle 1$ and $\langle 3 \rangle 2$

$\langle 5 \rangle 2.$ $|S| = \aleph_0 \vee |S| \in \mathbb{N}$, i.e. $S$ is countable

PROOF: By $\langle 5 \rangle 1$ (assuming a countable number of events)

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

PROOF: By $\langle 4 \rangle 1$ and $\langle 5 \rangle 2$, since $\sigma$-fields are closed under countable union.

$\langle 4 \rangle 3.$ $c(t_1) \setminus \bigcup\limits_{t \in S} c(t) \in \mathcal{F}_I$

PROOF: By $\langle 3 \rangle 1$ and $\langle 4 \rangle 2$, since $\sigma$-fields are closed under $\setminus$ (setminus).

$\langle 4 \rangle 4.$ $c(t_1) \setminus \bigcup\limits_{t \in S} c(t) = \{t_1\}$

$\langle 5 \rangle 1.$ $c(t_1) \setminus \bigcup\limits_{t \in S} c(t) \subseteq \{t_1\}$

$\langle 6 \rangle 1.$ ASSUME: $t_2 \in c(t_1) \setminus \bigcup\limits_{t \in S} c(t)$

PROVE: $t_2 \in \{t_1\}$, i.e. $t_2 = t_1$

$\langle 7 \rangle 1.$ ASSUME: $t_2 \neq t_1$

PROVE: $\perp$

$\langle 8 \rangle 1.$ $t_1 \sqsubseteq t_2$

PROOF: By assumption $\langle 6 \rangle 1$ ($t_2 \in c(t_1)$)

$\langle 8 \rangle 2.$ $\#t_2 > \#t_1$

PROOF: By assumption $\langle 7 \rangle 1$ and $\langle 8 \rangle 1$

$\langle 8 \rangle 3.$ $\exists t \in S : t_2 \in c(t)$

PROOF: By assumption $\langle 6\rangle 1$ ($t_2 \in c(t_1)$) and $\langle 8\rangle 2$

$\langle 8\rangle 4.$ $t_2 \in \bigcup_{t \in S} c(t)$

PROOF: By $\langle 8\rangle 3$

$\langle 8\rangle 5.$ Q.E.D.

PROOF: By assumption $\langle 6\rangle 1$ and $\langle 8\rangle 4$

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

PROOF: $\perp$-rule

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

PROOF: $\subseteq$-rule

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

$\langle 6\rangle 1.$ $t_1 \in c(t_1)$

PROOF: By assumption $\langle 1\rangle 1$ and definition 28

$\langle 6\rangle 2.$ $t_1 \notin \bigcup_{t \in S} c(t)$

$\langle 7\rangle 1.$ ASSUME: $t_1 \in \bigcup_{t \in S} c(t)$

PROVE: $\perp$

$\langle 8\rangle 1.$ LET: $t_2 \in S$ s.t. $t_1 \in c(t_2)$

PROOF: By assumption $\langle 7\rangle 1$

$\langle 8\rangle 2.$ $\forall t \in c(t_2) : \#t \geq \#t_2$

PROOF: By definition 28

$\langle 8\rangle 3.$ $\#t_2 = \#t_1 + 1$

PROOF: By $\langle 8\rangle 1$ and $\langle 3\rangle 2$

$\langle 8\rangle 4.$ $\forall t \in c(t_2) : \#t \geq \#t_1 + 1$

PROOF: By $\langle 8\rangle 2$ and $\langle 8\rangle 3$

$\langle 8\rangle 5.$ $\#t_1 \geq \#t_1 + 1$

PROOF: By $\langle 8\rangle 1$ ($t_1 \in c(t_2)$) and $\langle 8\rangle 4$

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

PROOF: By assumption $\langle 2\rangle 1$ and $\langle 8\rangle 5$

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

PROOF: $\perp$-rule

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

PROOF: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$

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

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

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

PROOF: By $\langle 4\rangle 3$ and $\langle 4\rangle 4$

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

PROOF: The cases $\langle 3\rangle 4$ and $\langle 3\rangle 5$ are exhaustive

$\langle 2\rangle 2.$ CASE: $\#t_1 = \infty$

$\langle 3\rangle 1.$ $\forall i \in \mathbb{N} : c(t_1|_i) \in \mathcal{F}_I$

$\langle 4\rangle 1.$ $\forall i \in \mathbb{N} : c(t_1|_i) \in C_I$

PROOF: By definition 29 and assumption $\langle 1\rangle 1$

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

PROOF: By $\langle 4\rangle 1$, since $C_I \subseteq \mathcal{F}_I$

$\langle 3\rangle 2.$ $\bigcap_{i=1}^{\infty} c(t_1|_i) \in \mathcal{F}_I$

PROOF: By $\langle 3\rangle 1$, since $\sigma$-fields are closed under countable intersection

$\langle 3\rangle 3.$ $\bigcap_{i=1}^{\infty} c(t_1|_i) = \{t_1\}$

PROOF: By assumption $\langle 1\rangle 1$ and definition 28

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

PROOF: By $\langle 3\rangle 2$ and $\langle 3\rangle 3$

$\langle 2\rangle 3.$ 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: $\forall$-rule

□

**Lemma 28.** *Let $d$ be a sequence diagram and $(traces(I), \mathcal{F}_I, f_I)$ be a probability space representing a system $I$. Then*

$$t \in traces(I) \Rightarrow \exists q \in [0,1] : ((\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\}), \{q\}) \in \langle I\rangle_d^p$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $t \in traces(I)$

PROVE: $\exists q \in [0,1] : ((\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\}), \{q\}) \in \langle I\rangle_d^p$

$\langle 2\rangle 1.$ $\{t\} \in \mathcal{F}_I$

PROOF: By assumption $\langle 1\rangle 1$ and Lemma 27

$\langle 2\rangle 2.$ $((\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\}), f_I(\{t\})) \in \langle I\rangle_d^p$

PROOF: By $\langle 2\rangle 1$ and definition 30

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

PROOF: By $\langle 2\rangle 2$; $f_I(\{t\})$ is the $q$ we are looking for

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

PROOF: $\Rightarrow$-rule

□

**Lemma 29.** *Let $O$ be a set of p-obligations. Then*

$$\forall S \subseteq O : S \neq \emptyset \Rightarrow \oplus O \rightsquigarrow_r \oplus S$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $S \subseteq O$

PROVE: $S \neq \emptyset \Rightarrow \oplus O \rightsquigarrow_r \oplus S$

$\langle 2\rangle 1.$ ASSUME: $S \neq \emptyset$

PROVE: $\oplus O \rightsquigarrow_r \oplus S$

$\langle 3\rangle 1.$ LET: $(p_1, n_1) = \oplus O$

$(p_2, n_2) = \oplus S$

$\langle 3\rangle 2.$ $p_1 \subseteq p_2 \cup n_2$

$\langle 4\rangle 1.$ ASSUME: $t \in p_1$

PROVE: $t \in p_2 \cup n_2$

⟨5⟩1. $t \in (\bigcup_{po \in O} p) \cap (\bigcap_{po \in O} (p \cup n))$
Proof: By assumption ⟨4⟩1

⟨5⟩2. $t \in \bigcap_{po \in O} (p \cup n)$
Proof: By ⟨5⟩1

⟨5⟩3. $t \in \bigcap_{po \in S} (p \cup n)$
Proof: By ⟨5⟩2 and assumption ⟨1⟩1

⟨5⟩4. Q.E.D.
Proof: By ⟨5⟩3

⟨4⟩2. Q.E.D.
Proof: $\subseteq$-rule

⟨3⟩3. $n_1 \subseteq n_2$

⟨4⟩1. Assume: $t \in n_1$
Prove: $t \in n_2$

⟨5⟩1. $t \in \bigcap_{po \in O} n$
Proof: By assumption ⟨4⟩1

⟨5⟩2. $t \in \bigcap_{po \in S} n$
Proof: By ⟨5⟩1 and assumption ⟨1⟩1

⟨5⟩3. Q.E.D.
Proof: By ⟨5⟩2

⟨4⟩2. Q.E.D.
Proof: $\subseteq$-rule

⟨3⟩4. Q.E.D.
Proof: By ⟨3⟩1, ⟨3⟩2 and ⟨3⟩3

⟨2⟩2. Q.E.D.
Proof: $\Rightarrow$-rule

⟨1⟩2. Q.E.D.
Proof: $\forall$-rule

□

**Lemma 30.** *Let $O$ be a set of p-obligations. Then*

$$\forall (o, Q) \in O : \oplus O \rightsquigarrow_r o$$

Proof.

⟨1⟩1. Assume: $(o, Q) \in O$
Prove: $\oplus O \rightsquigarrow_r o$

⟨2⟩1. Let: $S = \{(o, Q)\}$

⟨2⟩2. $S \subseteq O \land S \neq \emptyset$
Proof: By ⟨2⟩1 and assumption ⟨1⟩1

⟨2⟩3. $\oplus O \rightsquigarrow_r \oplus S$
Proof: By ⟨2⟩2 and Lemma 29

⟨2⟩4. $\oplus S = o$
Proof: By ⟨2⟩1 and definition 4

⟨2⟩5. Q.E.D.
PROOF: By ⟨2⟩3 and ⟨2⟩4

⟨1⟩2. Q.E.D.
PROOF: ∀-rule

□

**Lemma 31.**

$$\forall m \in \mathbb{N} : \sum_{j=1}^{m} \langle 0, 1] = \langle 0, 1]$$

PROOF.

⟨1⟩1. ASSUME: $m \in \mathbb{N}$
PROVE: $\sum_{j=1}^{m} \langle 0, 1] = \langle 0, 1]$

⟨2⟩1. CASE: $m = 1$

⟨3⟩1. $\sum_{j=1}^{1} \langle 0, 1] = \langle 0, 1]$
PROOF: By definition 7

⟨3⟩2. Q.E.D.
PROOF: By ⟨3⟩1 and assumption ⟨2⟩1

⟨2⟩2. CASE: $m > 1$

⟨3⟩1. ASSUME: $\sum_{j=1}^{m-1} \langle 0, 1] = \langle 0, 1]$ (ind.hyp.)
PROVE: $\sum_{j=1}^{m} \langle 0, 1] = \langle 0, 1]$

⟨4⟩1. $\sum_{j=1}^{m} \langle 0, 1] = (\sum_{j=1}^{m-1} \langle 0, 1]) + \langle 0, 1]$
PROOF: By definition 7

⟨4⟩2. $\sum_{j=1}^{m} \langle 0, 1] = \langle 0, 1] + \langle 0, 1]$
PROOF: By ⟨4⟩1 and assumption ⟨3⟩1

⟨4⟩3. $\langle 0, 1] + \langle 0, 1] = \langle 0, 1]$

⟨5⟩1. $\langle 0, 1] + \langle 0, 1] \subseteq \langle 0, 1]$

⟨6⟩1. ASSUME: $q \in \langle 0, 1] + \langle 0, 1]$
PROVE: $q \in \langle 0, 1]$

⟨7⟩1. LET: $q_1 \in \langle 0, 1], q_2 \in \langle 0, 1]$ s.t. $q = \mathsf{min}(q_1 + q_2, 1)$
PROOF: By assumption ⟨6⟩1

⟨7⟩2. CASE: $q_1 + q_2 < 1$

⟨8⟩1. $q = q_1 + q_2$
PROOF: By ⟨7⟩1 and assumption ⟨7⟩2

⟨8⟩2. $q_1 + q_2 > 0$
PROOF: By ⟨7⟩1

⟨8⟩3. Q.E.D.
PROOF: By ⟨8⟩1, ⟨8⟩2 and assumption ⟨7⟩2

⟨7⟩3. CASE: $q_1 + q_2 \geq 1$

$\langle 8\rangle$1. $q = 1$
PROOF: By assumption $\langle 7\rangle$3 and $\langle 7\rangle$1

$\langle 8\rangle$2. Q.E.D.
PROOF: By $\langle 8\rangle$1

$\langle 7\rangle$4. Q.E.D.
PROOF: The cases $\langle 7\rangle$2 and $\langle 7\rangle$3 are exhaustive

$\langle 6\rangle$2. Q.E.D.
PROOF: $\subseteq$-rule

$\langle 5\rangle$2. $\langle 0,1] \subseteq \langle 0,1] + \langle 0,1]$

$\langle 6\rangle$1. ASSUME: $q \in \langle 0,1]$
PROVE: $q \in \langle 0,1] + \langle 0,1]$

$\langle 7\rangle$1. LET: $q' = 0.5 * q$

$\langle 7\rangle$2. $q' \in \langle 0,1]$
PROOF: By assumption $\langle 6\rangle$1 and $\langle 7\rangle$1

$\langle 7\rangle$3. $q = q' + q'$
PROOF: By $\langle 7\rangle$1

$\langle 7\rangle$4. Q.E.D.
PROOF: By $\langle 7\rangle$2 and $\langle 7\rangle$3

$\langle 6\rangle$2. Q.E.D.
PROOF: $\subseteq$-rule

$\langle 5\rangle$3. Q.E.D.
PROOF: By $\langle 5\rangle$1 and $\langle 5\rangle$2

$\langle 4\rangle$4. Q.E.D.
PROOF: By $\langle 4\rangle$2 and $\langle 4\rangle$3

$\langle 3\rangle$2. Q.E.D.
PROOF: Induction step

$\langle 2\rangle$3. Q.E.D.
PROOF: By induction with $\langle 2\rangle$1 as base case and $\langle 2\rangle$2 as induction step

$\langle 1\rangle$2. Q.E.D.
PROOF: $\forall$-rule

□

**Lemma 32.** *Let $d \in \mathcal{D}^i$. Then*

$$\forall po \in [\![ \ g(d) \ ]\!]^p : Q = \{1\} \vee \langle 0,1] \subseteq Q$$

PROOF.

$\langle 1\rangle$1. ASSUME: $po \in [\![ \ g(d) \ ]\!]^p$
PROVE: $Q = \{1\} \vee \langle 0,1] \subseteq Q$

$\langle 2\rangle$1. CASE: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

$\langle 3\rangle$1. $[\![ \ g(d) \ ]\!]^p = \{ \ ((\{\langle e\rangle\},\emptyset),\{1\}) \ \} \vee [\![ \ g(d) \ ]\!]^p = \{ \ ((\{\langle\rangle\},\emptyset),\{1\}) \ \}$
PROOF: By assumption $\langle 2\rangle$1

$\langle 3\rangle$2. $po = ((\{\langle e\rangle\},\emptyset),\{1\}) \vee po = ((\{\langle\rangle\},\emptyset),\{1\})$
PROOF: By $\langle 3\rangle$1 and assumption $\langle 1\rangle$1

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

⟨2⟩2. CASE: $d$ contains at least one operator

⟨3⟩1. ASSUME: For every sub-diagram $d_j$ occurring in an operand of $d$ the following holds:
$\forall (o', Q') \in [\![ \; g(d_j) \; ]\!]^p : Q' = \{1\} \vee \langle 0, 1] \subseteq Q'$ (ind.hyp.)
PROVE: $Q = \{1\} \vee \langle 0, 1] \subseteq Q$

⟨4⟩1. CASE: $d = \mathsf{refuse}\ d_1$

⟨5⟩1. $g(d) = \mathsf{refuse}\ g(d_1)$
PROOF: By assumption ⟨4⟩1

⟨5⟩2. LET: $((p_1, n_1), Q_1) \in [\![ \; g(d_1) \; ]\!]^p$ s.t. $((p, n), Q) = ((\emptyset, p_1 \cup n_1), Q_1)$
PROOF: By assumption ⟨1⟩1 and ⟨5⟩1

⟨5⟩3. $Q_1 = \{1\} \vee \langle 0, 1] \subseteq Q_1$
PROOF: By ⟨5⟩2 and assumption ⟨3⟩1

⟨5⟩4. Q.E.D.
PROOF: By ⟨5⟩2 and ⟨5⟩3

⟨4⟩2. CASE: $d = d_1\ \mathsf{seq}\ d_2$

⟨5⟩1. $g(d) = g(d_1)\ \mathsf{seq}\ g(d_2)$
PROOF: By assumption ⟨4⟩2

⟨5⟩2. LET: $(o_1, Q_1) \in [\![ \; g(d_1) \; ]\!]^p, (o_1, Q_2) \in [\![ \; g(d_2) \; ]\!]^p$ s.t. $(o, Q) = (o_1 \succsim o_2, Q_1 * Q_2)$
PROOF: By assumption ⟨1⟩1 and ⟨5⟩1

⟨5⟩3. $(Q_1 = \{1\} \vee \langle 0, 1] \subseteq Q_1) \wedge (Q_2 = \{1\} \vee \langle 0, 1] \subseteq Q_2)$
PROOF: By ⟨5⟩2 and assumption ⟨3⟩1

⟨5⟩4. CASE: $Q_1 = \{1\} \wedge Q_2 = \{1\}$

⟨6⟩1. $Q_1 * Q_2 = \{1\}$
PROOF: By assumption ⟨5⟩4

⟨6⟩2. Q.E.D.
PROOF: By ⟨6⟩1 and ⟨5⟩2

⟨5⟩5. CASE: $Q_1 = \{1\} \wedge \langle 0, 1] \subseteq Q_2$

⟨6⟩1. $Q_1 * Q_2 = Q_2$
PROOF: By assumption ⟨5⟩5

⟨6⟩2. $\langle 0, 1] \subseteq Q_1 * Q_2$
PROOF: By ⟨6⟩1 and assumption ⟨5⟩5

⟨6⟩3. Q.E.D.
PROOF: By ⟨6⟩2 and ⟨5⟩2

⟨5⟩6. CASE: $\langle 0, 1] \subseteq Q_1 \wedge Q_2 = \{1\}$
PROOF: Similar to ⟨5⟩5

⟨5⟩7. CASE: $\langle 0, 1] \subseteq Q_1 \wedge \langle 0, 1] \subseteq Q_2$

⟨6⟩1. $\langle 0, 1] \subseteq Q_1 * Q_2$

⟨7⟩1. ASSUME: $q \in \langle 0, 1]$
PROVE: $q \in Q_1 * Q_2$

⟨8⟩1. $q \in Q_1$
PROOF: By assumption ⟨5⟩7 and assumption ⟨7⟩1

⟨8⟩2. $1 \in Q_2$
PROOF: By assumption ⟨5⟩7

⟨8⟩3. $q * 1 \in Q_1 * Q_2$

PROOF: By $\langle 8\rangle 1$ and $\langle 8\rangle 2$

$\langle 8\rangle 4$. Q.E.D.

PROOF: By $\langle 8\rangle 3$

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

PROOF: $\subseteq$-rule

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

PROOF: By $\langle 6\rangle 1$ and $\langle 5\rangle 2$

$\langle 5\rangle 8$. Q.E.D.

PROOF: By $\langle 5\rangle 3$ the cases $\langle 5\rangle 4$, $\langle 5\rangle 5$, $\langle 5\rangle 6$ and $\langle 5\rangle 7$ are exhaustive

$\langle 4\rangle 3$. CASE: $d = d_1 \text{ par } d_2$

PROOF: Similar to case $\langle 4\rangle 2$

$\langle 4\rangle 4$. CASE: $d = d_1 \text{ alt } d_2$

PROOF: Similar to case $\langle 4\rangle 2$

$\langle 4\rangle 5$. CASE: $d = \mathsf{xalt}(d_1, \dots, d_m)$

$\langle 5\rangle 1$. $g(d) = \mathsf{palt}(g(d_1);\langle 0,1] , \dots , g(d_m);\langle 0,1])$

PROOF: By assumption $\langle 4\rangle 5$

$\langle 5\rangle 2$. CASE: $po \in \{(\oplus \bigcup_{j\in N} \{po_j\}, \sum_{j\in N} Q_j) \mid N \subseteq \{1, \dots, m\} \wedge N \neq \emptyset \wedge \forall j \in N : po_j \in [\![\ g(d_j);\langle 0,1]\ ]\!]^p\}$

$\langle 6\rangle 1$. LET: $N \subseteq \{1, \dots, m\}$ s.t. $po = (\oplus \bigcup_{j\in N} \{po_j\}, \sum_{j\in N} Q_j) \wedge N \neq \emptyset \wedge \forall j \in N : po_j \in [\![\ g(d_j);\langle 0,1]\ ]\!]^p$

PROOF: By assumption $\langle 5\rangle 2$

$\langle 6\rangle 2$. LET: $Q'_j \subseteq [0,1]$ s.t. $(o_j, Q_j) = (o_j, Q'_j * \langle 0,1]) \wedge (o_j, Q'_j) \in [\![\ g(d_j)\ ]\!]^p$ for each $j \in N$

PROOF: By $\langle 6\rangle 1$

$\langle 6\rangle 3$. $\forall j \in N : \langle 0,1] \subseteq Q_j$

$\langle 7\rangle 1$. $\forall j \in N : Q'_j = \{1\} \vee \langle 0,1] \subseteq Q'_j$

PROOF: By $\langle 6\rangle 2$ and assumption $\langle 3\rangle 1$

$\langle 7\rangle 2$. $\{1\} * \langle 0,1] = \langle 0,1] * \langle 0,1] = \langle 0,1]$

PROOF: By definition 2

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

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 6\rangle 2$ ($Q_j = Q'_j * \langle 0,1]$ for each $j \in N$)

$\langle 6\rangle 4$. $\langle 0,1] \subseteq \sum_{j\in N} Q_j$

PROOF: By $\langle 6\rangle 3$ and Lemma 31

$\langle 6\rangle 5$. Q.E.D.

PROOF: By $\langle 6\rangle 4$ and $\langle 6\rangle 1$ ($Q = \sum_{j\in N} Q_j$)

$\langle 5\rangle 3$. CASE: $po = (\oplus \bigcup_{j=1}^{m} [\![\ d_j;\langle 0,1]\ ]\!]^p, \{1\} \cap \sum_{j=1}^{m} \langle 0,1])$

$\langle 6\rangle 1$. $\sum_{j=1}^{m} \langle 0,1] = \langle 0,1]$

PROOF: By Lemma 31

$\langle 6\rangle 2$. $\{1\} \cap \sum_{j=1}^{m} \langle 0,1] = \{1\}$

PROOF: By $\langle 6\rangle 1$

⟨6⟩3. Q.E.D.

Proof: By ⟨6⟩2 and assumption ⟨5⟩3 ($Q = \{1\} \cap \sum_{j=1}^{m} \langle 0, 1]$)

⟨5⟩4. Q.E.D.

Proof: By ⟨5⟩1 the cases ⟨5⟩2 and ⟨5⟩3 are exhaustive

⟨4⟩6. Q.E.D.

Proof: The cases ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 and ⟨4⟩5 are exhaustive

⟨3⟩2. Q.E.D.

Proof: Induction step

⟨2⟩3. Q.E.D.

Proof: By induction with ⟨2⟩1 as base case and ⟨2⟩2 as induction step

⟨1⟩2. Q.E.D.

Proof: ∀-rule

□

**Lemma 33.** *Let $d \in \mathcal{D}^i$. Then*

$$(o, \{1\}) \in [\![\ g(d)\ ]\!]^p \Rightarrow \forall (o', Q') \in [\![\ g(d)\ ]\!]^p : o \rightsquigarrow_r o'$$

Proof.

⟨1⟩1. Assume: $(o, \{1\}) \in [\![\ g(d)\ ]\!]^p$

Prove: $\forall (o', Q') \in [\![\ g(d)\ ]\!]^p : o \rightsquigarrow_r o'$

⟨2⟩1. Assume: $(o', Q') \in [\![\ g(d)\ ]\!]^p$

Prove: $o \rightsquigarrow_r o'$

⟨3⟩1. Case: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

⟨4⟩1. $[\![\ g(d)\ ]\!]^p = \{\ ((\{\langle e\rangle\}, \emptyset), \{1\})\ \} \vee [\![\ g(d)\ ]\!]^p = \{\ ((\{\langle\rangle\}, \emptyset), \{1\})\ \}$

Proof: By assumption ⟨3⟩1

⟨4⟩2. $(o, \{1\}) = (o', Q')$

Proof: By assumption ⟨1⟩1, assumption ⟨2⟩1 and ⟨4⟩1

⟨4⟩3. Q.E.D.

Proof: By ⟨4⟩2, since $o \rightsquigarrow_r o$ for any $o$

⟨3⟩2. Case: $d$ contains at least one operator

⟨4⟩1. Assume: For every sub-diagram $d_j$ occurring in an operand of $d$ the following holds:
$(o_j, \{1\}) \in [\![\ g(d_j)\ ]\!]^p \Rightarrow \forall (o'_j, Q'_j) \in [\![\ g(d_j)\ ]\!]^p : o_j \rightsquigarrow_r o'_j$
(ind.hyp.)

Prove: $o \rightsquigarrow_r o'$

⟨5⟩1. Case: $d = \mathsf{refuse}\ d_1$

⟨6⟩1. Let: $((p_1, n_1), \{1\}) \in [\![\ g(d_1)\ ]\!]^p$ s.t. $o = (\emptyset, p_1 \cup n_1)$

Proof: By assumption ⟨1⟩1 and assumption ⟨5⟩1

⟨6⟩2. Let: $((p'_1, n'_1), Q'_1) \in [\![\ g(d_1)\ ]\!]^p$ s.t. $(o', Q') = ((\emptyset, p'_1 \cup n'_1), Q'_1)$

Proof: By assumption ⟨2⟩1 and assumption ⟨5⟩1

⟨6⟩3. $(p_1, n_1) \rightsquigarrow_r (p'_1, n'_1)$

Proof: By ⟨6⟩1, ⟨6⟩2 and assumption ⟨4⟩1

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩3 and Lemma 4 in [RHS07b]

$\langle 5 \rangle 2$. CASE: $d = d_1$ $\mathsf{seq}$ $d_2$

$\langle 6 \rangle 1$. LET: $(o_1, \{1\}) \in \llbracket\, g(d_1)\, \rrbracket^p, (o_2, \{1\}) \in \llbracket\, g(d_2)\, \rrbracket^p$ s.t.
$o = o_1 \succsim o_2$

PROOF: By assumption $\langle 1 \rangle 1$ and assumption $\langle 5 \rangle 2$

$\langle 6 \rangle 2$. LET: $(o_1', Q_1') \in \llbracket\, g(d_1)\, \rrbracket^p, (o_2', Q_2') \in \llbracket\, g(d_2)\, \rrbracket^p$ s.t.
$(o', Q') = (o_1' \succsim o_2', Q_1' * Q_2')$

PROOF: By assumption $\langle 2 \rangle 1$ and assumption $\langle 5 \rangle 2$

$\langle 6 \rangle 3$. $o_1 \rightsquigarrow_r o_1' \wedge o_2 \rightsquigarrow_r o_2'$

PROOF: By $\langle 6 \rangle 1$, $\langle 6 \rangle 2$ and assumption $\langle 4 \rangle 1$

$\langle 6 \rangle 4$. Q.E.D.

PROOF: By $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$ and Lemma 30 in [HHRS06]

$\langle 5 \rangle 3$. CASE: $d = d_1$ $\mathsf{par}$ $d_2$

PROOF: Similar to case $\langle 5 \rangle 2$; refer to Lemma 31 in [HHRS06] instead of Lemma 30 in [HHRS06]

$\langle 5 \rangle 4$. CASE: $d = d_1$ $\mathsf{alt}$ $d_2$

PROOF: Similar to case $\langle 5 \rangle 2$; refer to Theorem 11 in [RRS07] instead of Lemma 30 in [HHRS06]

$\langle 5 \rangle 5$. CASE: $d = \mathsf{xalt}(d_1 \ldots, d_m)$

$\langle 6 \rangle 1$. $g(d) = \mathsf{palt}(g(d_1);\langle 0,1]\,, \ldots, g(d_m);\langle 0,1])$

PROOF: By assumption $\langle 5 \rangle 5$

$\langle 6 \rangle 2$. $o = \oplus \bigcup_{i=1}^{m} \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p$

$\langle 7 \rangle 1$. $\forall Q \subseteq [0,1] : Q * \langle 0,1] \neq \{1\}$

PROOF: By definition 2

$\langle 7 \rangle 2$. $\forall (o_j, Q_j) \in \bigcup_{i=1}^{m} \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p : Q_j \neq \{1\}$

PROOF: By $\langle 7 \rangle 1$

$\langle 7 \rangle 3$. $\bigcup_{i=1}^{m} \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p \subseteq \llbracket\, g(d)\, \rrbracket^p$

PROOF: By $\langle 6 \rangle 1$ and definition 9

$\langle 7 \rangle 4$. $\forall (o_j, Q_j) \in \bigcup_{i=1}^{m} \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p : \langle 0,1] \subseteq Q_j$

PROOF: By $\langle 7 \rangle 2$, $\langle 7 \rangle 3$ and Lemma 32

$\langle 7 \rangle 5$. $\forall S \subseteq \bigcup_{i=1}^{m} \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p : \sum_{(o_j, Q_j) \in S} Q_j \neq \{1\}$

PROOF: By $\langle 7 \rangle 4$

$\langle 7 \rangle 6$. Q.E.D.

PROOF: By assumption $\langle 1 \rangle 1$, $\langle 7 \rangle 5$ and definition 9 (by $\langle 7 \rangle 5$, $(o, \{1\})$ must result from line $b$ in definition 9)

$\langle 6 \rangle 3$. CASE: $po' = (\oplus \bigcup_{i=1}^{m} \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p, \{1\} \cap \sum_{i=1}^{m} \langle 0,1])$

$\langle 7 \rangle 1$. Q.E.D.

PROOF: By $\langle 6 \rangle 2$ and assumption $\langle 6 \rangle 3$

$\langle 6 \rangle 4$. CASE: $po' \in \{(\oplus \bigcup_{i \in N} \{po_i\}, \sum_{i \in N} \pi_2.po_i) \mid N \subseteq \{1, \ldots, m\} \wedge N \neq \emptyset \wedge \forall i \in N : po_i \in \llbracket\, g(d_i);\langle 0,1]\, \rrbracket^p\}$

$\langle 7\rangle 1.$ Let: $S \subseteq \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p$ s.t. $S \neq \emptyset \wedge o' = \oplus S$
Proof: By assumption $\langle 6\rangle 4$

$\langle 7\rangle 2.$ $\oplus \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p \rightsquigarrow_r \oplus S$
Proof: By $\langle 7\rangle 1$ and Lemma 29

$\langle 7\rangle 3.$ $o \rightsquigarrow \oplus S$
Proof: By $\langle 7\rangle 2$ and $\langle 6\rangle 2$

$\langle 7\rangle 4.$ Q.E.D.
Proof: By $\langle 7\rangle 3$ and $\langle 7\rangle 1$ ($o' = \oplus S$)

$\langle 6\rangle 5.$ Q.E.D.
Proof: By $\langle 6\rangle 1$ the cases $\langle 6\rangle 3$ and $\langle 6\rangle 4$ are exhaustive

$\langle 5\rangle 6.$ Q.E.D.
Proof: The cases $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$ and $\langle 5\rangle 5$ are exhaustive

$\langle 4\rangle 2.$ Q.E.D.
Proof: Induction step

$\langle 3\rangle 3.$ Q.E.D.
Proof: By induction with $\langle 3\rangle 1$ as base case and $\langle 3\rangle 2$ as induction step

$\langle 2\rangle 2.$ Q.E.D.
Proof: $\forall$-rule

$\langle 1\rangle 2.$ Q.E.D.
Proof: $\Rightarrow$-rule

□

Note that Lemma 33 holds only for sequence diagrams on the form $g(d)$, and not for sequence diagrams in general.

**Lemma 34.** *Let $d \in \mathcal{D}^i$. Then*

$$[\![\ d\ ]\!]^i \subseteq \{o \mid (o,Q) \in [\![\ g(d)\ ]\!]^p\}$$

Proof.

$\langle 1\rangle 1.$ $\forall o \in [\![\ d\ ]\!]^i : \exists Q \subseteq [0,1] : (o,Q) \in [\![\ g(d)\ ]\!]^p$

$\langle 2\rangle 1.$ Assume: $o_1 \in [\![\ d\ ]\!]^i$
Prove: $\exists Q \subseteq [0,1] : (o_1,Q) \in [\![\ g(d)\ ]\!]^p$

$\langle 3\rangle 1.$ Case: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

$\langle 4\rangle 1.$ Case: $d$ consists of a single event $e$

$\langle 5\rangle 1.$ $[\![\ d\ ]\!]^i = \{\ (\{\langle e\rangle\},\emptyset)\ \} \wedge [\![\ g(d)\ ]\!]^p = \{\ ((\{\langle e\rangle\},\emptyset),\{1\})\ \}$
Proof: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ Q.E.D.
Proof: By $\langle 5\rangle 1$; $\{1\}$ is the $Q$ we are looking for

$\langle 4\rangle 2.$ Case: $d = \mathsf{skip}$
Proof: Similar to $\langle 4\rangle 2$; just replace $\langle e\rangle$ with $\langle\rangle$

$\langle 4\rangle 3.$ Q.E.D.
Proof: By $\langle 3\rangle 1$ the cases $\langle 4\rangle 1$ and $\langle 4\rangle 2$ are exhaustive

$\langle 3\rangle 2.$ Case: $d$ contains at least one operator

$\langle 4\rangle 1.$ ASSUME: For every sub-diagram $d_j$ occurring in an operand of $d$ the following holds:
$\forall o \in \llbracket\ d_j\ \rrbracket^i : \exists Q \subseteq [0,1] : (o,Q) \in \llbracket\ g(d_j)\ \rrbracket^p$ (ind.hyp.)
PROVE: $\exists Q \subseteq [0,1] : (o_1, Q) \in \llbracket\ g(d)\ \rrbracket^p$

$\langle 5\rangle 1.$ CASE: $d = \mathsf{refuse}\ d_1$

$\langle 6\rangle 1.$ LET: $(p'_1, n'_1) \in \llbracket\ d_1\ \rrbracket^i$ s.t. $o_1 = (\emptyset, p'_1 \cup n'_1)$
PROOF: By assumption $\langle 2\rangle 1$ and assumption $\langle 5\rangle 1$

$\langle 6\rangle 2.$ LET: $Q'_1 \subseteq [0,1]$ s.t. $((p'_1, n'_1), Q'_1) \in \llbracket\ g(d_1)\ \rrbracket^p$
PROOF: By $\langle 6\rangle 1$ and assumption $\langle 4\rangle 1$

$\langle 6\rangle 3.$ $((\emptyset, p'_1 \cup n'_1), Q'_1) \in \llbracket\ g(d)\ \rrbracket^p$

$\langle 7\rangle 1.$ $g(d) = \mathsf{refuse}\ g(d_1)$
PROOF: By assumption $\langle 5\rangle 1$ and definition 38

$\langle 7\rangle 2.$ Q.E.D.
PROOF: By $\langle 7\rangle 1$ and $\langle 6\rangle 2$ $(((p'_1, n'_1), Q'_1) \in \llbracket\ g(d_1)\ \rrbracket^p)$

$\langle 6\rangle 4.$ Q.E.D.
PROOF: By $\langle 6\rangle 3$ and $\langle 6\rangle 1$ $(o_1 = (\emptyset, p'_1 \cup n'_1))$; $Q'_1$ is the $Q$ we are looking for

$\langle 5\rangle 2.$ CASE: $d = d_1\ \mathsf{seq}\ d_2$

$\langle 6\rangle 1.$ LET: $o'_1 \in \llbracket\ d_1\ \rrbracket^i, o'_2 \in \llbracket\ d_2\ \rrbracket^i$ s.t. $o_1 = o'_1 \succsim o'_2$
PROOF: By assumption $\langle 2\rangle 1$ and assumption $\langle 5\rangle 2$

$\langle 6\rangle 2.$ LET: $Q'_1 \subseteq [0,1]$ s.t. $(o'_1, Q'_1) \in \llbracket\ g(d_1)\ \rrbracket^p$
$Q'_2 \subseteq [0,1]$ s.t. $(o'_2, Q'_2) \in \llbracket\ g(d_2)\ \rrbracket^p$
PROOF: By $\langle 6\rangle 1$ and assumption $\langle 4\rangle 1$

$\langle 6\rangle 3.$ $(o'_1 \succsim o'_2, Q'_1 * Q'_2) \in \llbracket\ g(d)\ \rrbracket^p$

$\langle 7\rangle 1.$ $g(d) = g(d_1)\ \mathsf{seq}\ g(d_2)$
PROOF: By assumption $\langle 5\rangle 2$ and definition 38

$\langle 7\rangle 2.$ Q.E.D.
PROOF: By $\langle 7\rangle 1$ and $\langle 6\rangle 2$ $((o'_1, Q'_1) \in \llbracket\ g(d_1)\ \rrbracket^p \wedge (o'_2, Q'_2) \in \llbracket\ g(d_2)\ \rrbracket^p)$

$\langle 6\rangle 4.$ Q.E.D.
PROOF: By $\langle 6\rangle 3$ and $\langle 6\rangle 1$ $(o_1 = o'_1 \succsim o'_2)$; $Q'_1 * Q'_2$ is the $Q$ we are looking for

$\langle 5\rangle 3.$ CASE: $d = d_1\ \mathsf{par}\ d_2$
PROOF: Similar to case $\langle 5\rangle 2$

$\langle 5\rangle 4.$ CASE: $d = d_1\ \mathsf{alt}\ d_2$
PROOF: Similar to case $\langle 5\rangle 2$

$\langle 5\rangle 5.$ CASE: $d = \mathsf{xalt}(d_1, \ldots, d_m)$

$\langle 6\rangle 1.$ $o_1 \in \bigcup_{j=1}^{m} \llbracket\ d_j\ \rrbracket^i$
PROOF: By assumption $\langle 2\rangle 1$ and assumption $\langle 5\rangle 5$

$\langle 6\rangle 2.$ LET: $k \in \{1, \ldots, m\}$ s.t. $o_1 \in \llbracket\ d_k\ \rrbracket^i$
PROOF: By $\langle 6\rangle 1$

$\langle 6\rangle 3.$ LET: $Q_k \subseteq [0,1]$ s.t. $(o_1, Q_k) \in \llbracket\ g(d_k)\ \rrbracket^p$
PROOF: By assumption $\langle 6\rangle 2$ and assumption $\langle 4\rangle 1$

$\langle 6\rangle 4.$ $(o_1, Q_k * \langle 0,1])\in \llbracket\ g(d)\ \rrbracket^p$

$\langle 7\rangle 1.$ $g(d) = \mathsf{palt}(g(d_1);\langle 0,1], \ldots, g(d_2);\langle 0,1])$
PROOF: By assumption $\langle 5\rangle 5$ and definition 38

$\langle 7\rangle 2.$ Q.E.D.
PROOF: By $\langle 6\rangle 3$ ($(o_1, Q_k) \in \llbracket\ g(d_k)\ \rrbracket^p$), $\langle 7\rangle 1$ and definition 9 (from line (a) with $N = \{1\}$)

$\langle 6\rangle 5.$ Q.E.D.
PROOF: By $\langle 6\rangle 4$; $Q_k * \langle 0,1]$ is the $Q$ we are looking for

$\langle 5\rangle 6.$ Q.E.D.
PROOF: The cases $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$ and $\langle 5\rangle 5$ are exhaustive

$\langle 4\rangle 2.$ Q.E.D.
PROOF: Induction step

$\langle 3\rangle 3.$ Q.E.D.
PROOF: By induction with $\langle 3\rangle 1$ as base case and $\langle 3\rangle 2$ as induction step

$\langle 2\rangle 2.$ Q.E.D.
PROOF: $\forall$-rule

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

□

**Lemma 35.** *Let $d \in \mathcal{D}^i$. Then*

$$\forall (o, Q) \in \llbracket\ g(d)\ \rrbracket^p : \exists o' \in \llbracket\ d\ \rrbracket^i : o \rightsquigarrow_r o'$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $(o, Q) \in \llbracket\ g(d)\ \rrbracket^p$
PROVE: $\exists o' \in \llbracket\ d\ \rrbracket^i : o \rightsquigarrow_r o'$

$\langle 2\rangle 1.$ CASE: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

$\langle 3\rangle 1.$ CASE: $d$ consists of a single event $e$

$\langle 4\rangle 1.$ $\llbracket\ d\ \rrbracket^i = \{\ (\{\langle e\rangle\}, \emptyset)\ \} \wedge \llbracket\ g(d)\ \rrbracket^p = \{\ ((\{\langle e\rangle\}, \emptyset), \{1\})\ \}$
PROOF: By assumption $\langle 3\rangle 1$

$\langle 4\rangle 2.$ Q.E.D.
PROOF: By $\langle 4\rangle 1$; $(\{\langle e\rangle\}, \emptyset)$ is the $o'$ we are looking for

$\langle 3\rangle 2.$ CASE: $d = \mathsf{skip}$
PROOF: Similar to $\langle 3\rangle 1$; just replace $\langle e\rangle$ with $\langle\rangle$

$\langle 3\rangle 3.$ Q.E.D.
PROOF: By $\langle 2\rangle 1$ the cases $\langle 3\rangle 1$ and $\langle 3\rangle 2$ are exhaustive

$\langle 2\rangle 2.$ CASE: $d$ contains at least one operator

$\langle 3\rangle 1.$ ASSUME: For every sub-diagram $d_j$ occurring in an operand of $d$ the following holds:
$\forall (o'', Q'') \in \llbracket\ g(d_j)\ \rrbracket^p : \exists o' \in \llbracket\ d_j\ \rrbracket^i : o'' \rightsquigarrow_r o'$ (ind.hyp.)
PROVE: $\exists o' \in \llbracket\ d\ \rrbracket^i : o \rightsquigarrow_r o'$

$\langle 4\rangle 1.$ CASE: $d = \mathsf{refuse}\ d_1$

$\langle 5\rangle 1.$ LET: $((p_1, n_1), Q_1) \in \llbracket\ g(d_1)\ \rrbracket^p$ s.t. $(o, Q) = ((\emptyset, p_1 \cup n_1), Q_1)$
PROOF: By assumption $\langle 1\rangle 1$ and assumption $\langle 4\rangle 1$

$\langle 5\rangle 2.$ LET: $(p'_1, n'_1) \in \llbracket\ d_1\ \rrbracket^i$ s.t. $(p_1, n_1) \rightsquigarrow_r (p'_1, n'_1)$
PROOF: By $\langle 5\rangle 1$ and assumption $\langle 3\rangle 1$

⟨5⟩3. $(\emptyset, p_1 \cup n_1) \rightsquigarrow_r (\emptyset, p_1' \cup n_1')$

Proof: By ⟨5⟩2 and Lemma 4 in [RHS07b]

⟨5⟩4. $(\emptyset, p_1' \cup n_1') \in \llbracket\ d\ \rrbracket^i$

Proof: By assumption ⟨4⟩1 and ⟨5⟩2

⟨5⟩5. Q.E.D.

Proof: By ⟨5⟩3, ⟨5⟩4 and ⟨5⟩1 ($o = (\emptyset, p_1 \cup n_1)$); $(\emptyset, p_1' \cup n_1')$ is the $o'$ we are looking for

⟨4⟩2. Case: $d = d_1\ \mathsf{seq}\ d_2$

⟨5⟩1. Let: $(o_1, Q_1) \in \llbracket\ g(d_1)\ \rrbracket^p, (o_2, Q_2) \in \llbracket\ g(d_2)\ \rrbracket^p$ s.t. $(o, Q) = (o_1 \succsim o_2, Q_1 * Q_2)$

Proof: By assumption ⟨1⟩1 and assumption ⟨4⟩2

⟨5⟩2. Let: $o_1' \in \llbracket\ d_1\ \rrbracket^i$ s.t. $o_1 \rightsquigarrow_r o_1'$
$o_2' \in \llbracket\ d_2\ \rrbracket^i$ s.t. $o_2 \rightsquigarrow_r o_2'$

Proof: By ⟨5⟩1 and assumption ⟨3⟩1

⟨5⟩3. $o_1 \succsim o_2 \rightsquigarrow_r o_1' \succsim o_2'$

Proof: By ⟨5⟩2 and Lemma 30 in [HHRS06]

⟨5⟩4. $o_1' \succsim o_2' \in \llbracket\ d\ \rrbracket^i$

Proof: By assumption ⟨4⟩2 and ⟨5⟩2

⟨5⟩5. Q.E.D.

Proof: By ⟨5⟩3, ⟨5⟩4 and ⟨5⟩1 ($o = o_1 \succsim o_2$); $o_1' \succsim o_2'$ is the $o'$ we are looking for

⟨4⟩3. Case: $d = d_1\ \mathsf{par}\ d_2$

Proof: Similar to case ⟨4⟩2 (replace the reference to Lemma 30 in [HHRS06] with a reference to Lemma 31 in [HHRS06])

⟨4⟩4. Case: $d = d_1\ \mathsf{alt}\ d_2$

Proof: Similar to case ⟨4⟩2 (replace the reference to Lemma 30 in [HHRS06] with a reference to Theorem 11 in [RRS07])

⟨4⟩5. Case: $d = \mathsf{xalt}(d_1, \ldots, d_m)$

⟨5⟩1. $g(d) = \mathsf{palt}(g(d_1);\langle 0, 1], \ldots, g(d_m);\langle 0, 1])$

Proof: By assumption ⟨4⟩5

⟨5⟩2. Case: $(o, Q) = (\oplus \bigcup_{i \in N} \{po_i\}, \sum_{i \in N} \pi_2.po_i)$, where $N \subseteq \{1, \ldots, m\} \wedge N \neq \emptyset \wedge \forall i \in N : po_i \in \llbracket\ g(d_i);\langle 0, 1]\ \rrbracket^p$

⟨6⟩1. Let: $j \in N$ and $po_j \in \llbracket\ g(d_j);\langle 0, 1]\ \rrbracket^p$ s.t. $po_j \in \bigcup_{i \in N} \{po_i\}$

Proof: By assumption ⟨5⟩2 ($N \neq \emptyset \wedge \forall i \in N : po_i \in \llbracket\ g(d_i);\langle 0, 1]\ \rrbracket^p$)

⟨6⟩2. Let: $po_j^a \in \llbracket\ g(d_j)\ \rrbracket^p$ s.t. $o_j^a = o_j$

Proof: By ⟨6⟩1 ($po_j \in \llbracket\ g(d_j);\langle 0, 1]\ \rrbracket^p$)

⟨6⟩3. Let: $o_j' \in \llbracket\ d_j\ \rrbracket^i$ s.t. $o_j^a \rightsquigarrow_r o_j'$

Proof: By ⟨6⟩2 and assumption ⟨3⟩1

⟨6⟩4. $o_j \rightsquigarrow_r o_j'$

Proof: By ⟨6⟩3 and ⟨6⟩2

⟨6⟩5. $\oplus \bigcup_{i \in N} \{po_i\} \rightsquigarrow_r o_j'$

⟨7⟩1. $\oplus \bigcup_{i \in N} \{po_i\} \rightsquigarrow_r o_j$

Proof: By ⟨6⟩1 ($po_j \in \bigcup_{i \in N} \{po_i\}$) and Lemma 30

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

PROOF: By $\langle 7\rangle 1$, $\langle 6\rangle 4$ and Lemma 26 in [HHRS06]

$\langle 6\rangle 6$. $o'_j \in [\![\ d\ ]\!]^i$

PROOF: By $\langle 6\rangle 3$ ($o'_j \in [\![\ d_j\ ]\!]^i$) and assumption $\langle 4\rangle 5$

$\langle 6\rangle 7$. Q.E.D.

PROOF: By $\langle 5\rangle 2$ ($o = \oplus \bigcup_{i\in N} \{po_i\}$), $\langle 6\rangle 5$ and $\langle 6\rangle 6$; $o'_j$ is the $o'$ we are looking for

$\langle 5\rangle 3$. CASE: $(o, Q) = (\oplus \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p, \{1\} \cap \sum_{i=1}^{m} \langle 0,1])$

$\langle 6\rangle 1$. LET: $(o_1, Q_1) \in [\![\ g(d_1)\ ]\!]^p$

$\langle 6\rangle 2$. LET: $o'_1 \in [\![\ d_1\ ]\!]^i$ s.t. $o_1 \rightsquigarrow_r o'_1$

PROOF: By $\langle 6\rangle 1$ and assumption $\langle 3\rangle 1$

$\langle 6\rangle 3$. $(o_1, Q_1 * \langle 0,1]) \in \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p$

PROOF: By $\langle 6\rangle 1$

$\langle 6\rangle 4$. $\oplus \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p \rightsquigarrow_r o_1$

PROOF: By $\langle 6\rangle 3$ and Lemma 30

$\langle 6\rangle 5$. $\oplus \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p \rightsquigarrow_r o'_1$

PROOF: By $\langle 6\rangle 2$, $\langle 6\rangle 4$ and Lemma 26 in [HHRS06]

$\langle 6\rangle 6$. $o'_1 \in [\![\ d\ ]\!]^i$

PROOF: By $\langle 6\rangle 2$ ($o'_1 \in [\![\ d_1\ ]\!]^i$) and assumption $\langle 4\rangle 5$

$\langle 6\rangle 7$. Q.E.D.

PROOF: By $\langle 6\rangle 5$, $\langle 6\rangle 6$ and assumption $\langle 5\rangle 3$ ($o = (\oplus \bigcup_{i=1}^{m} [\![\ g(d_i);\langle 0,1]\ ]\!]^p)$; $o'_1$ is the $o'$ we are looking for

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

PROOF: By $\langle 5\rangle 1$ and definition 9 the cases $\langle 5\rangle 2$ and $\langle 5\rangle 3$ are exhaustive

$\langle 4\rangle 6$. Q.E.D.

PROOF: The cases $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$ and $\langle 4\rangle 5$ are exhaustive

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

PROOF: Induction step

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

PROOF: By induction with $\langle 2\rangle 1$ as base case and $\langle 2\rangle 2$ as induction step

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

PROOF: $\forall$-rule

□

**Lemma 36.** *Let $d \in \mathcal{D}^i$. Then*

$$\exists (o, Q) \in [\![\ g(d)\ ]\!]^p : Q = \{1\}$$

PROOF.

$\langle 1\rangle 1$. CASE: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

⟨2⟩1. $\llbracket\ g(d)\ \rrbracket^p = \{\ ((\{\langle e\rangle\},\emptyset),\{1\})\ \} \vee \llbracket\ g(d)\ \rrbracket^p = \{\ ((\{\langle\rangle\},\emptyset),\{1\})\ \}$

Proof: By assumption ⟨1⟩1

⟨2⟩2. Q.E.D.

Proof: By ⟨2⟩1

⟨1⟩2. Case: $d$ contains at least one operator

⟨2⟩1. Assume: For every sub-diagram $d_j$ occurring in an operand of $d$ the following holds:
$\exists(o_j,Q_j) \in \llbracket\ g(d_j)\ \rrbracket^p : Q_j = \{1\}$ (ind.hyp.)

Prove: $\exists(o,Q) \in \llbracket\ g(d)\ \rrbracket^p : Q = \{1\}$

⟨3⟩1. Case: $d = \mathsf{refuse}\ d_1$

⟨4⟩1. $g(d) = \mathsf{refuse}\ g(d_1)$

Proof: By assumption ⟨3⟩1

⟨4⟩2. Let: $((p_1,n_1),Q_1) \in \llbracket\ g(d_1)\ \rrbracket^p$ s.t. $Q_1 = \{1\}$

Proof: By assumption ⟨3⟩1 and assumption ⟨2⟩1

⟨4⟩3. $((\emptyset,n_1 \cup p_1),Q_1) \in \llbracket\ g(d)\ \rrbracket^p$

Proof: By ⟨4⟩2 and ⟨4⟩1

⟨4⟩4. Q.E.D.

Proof: By ⟨4⟩3 and ⟨4⟩2

⟨3⟩2. Case: $d = d_1\ \mathsf{seq}\ d_2$

⟨4⟩1. $g(d) = g(d_1)\ \mathsf{seq}\ g(d_2)$

Proof: By assumption ⟨3⟩2

⟨4⟩2. Let: $(o_1,Q_1) \in \llbracket\ g(d_1)\ \rrbracket^p$ s.t. $Q_1 = \{1\}$
$(o_2,Q_2) \in \llbracket\ g(d_2)\ \rrbracket^p$ s.t. $Q_2 = \{1\}$

Proof: By assumption ⟨3⟩2 and assumption ⟨2⟩1

⟨4⟩3. $(o_1 \succsim o_2, \{1\} * \{1\}) \in \llbracket\ g(d)\ \rrbracket^p$

Proof: By ⟨4⟩2 and ⟨4⟩1

⟨4⟩4. Q.E.D.

Proof: By ⟨4⟩3, since $\{1\} * \{1\} = \{1\}$

⟨3⟩3. Case: $d = d_1\ \mathsf{par}\ d_2$

Proof: Similar to case ⟨3⟩2

⟨3⟩4. Case: $d = d_1\ \mathsf{alt}\ d_2$

Proof: Similar to case ⟨3⟩2

⟨3⟩5. Case: $d = \mathsf{xalt}(d_1,\ldots,d_m)$

⟨4⟩1. $g(d) = \mathsf{palt}(g(d_1);\langle 0,1],\ldots,g(d_m);\langle 0,1])$

Proof: By assumption ⟨3⟩5

⟨4⟩2. $(\oplus \bigcup_{j=1}^{m} \llbracket\ g(d_j);\langle 0,1]\ \rrbracket, \{1\} \cap \sum_{j=1}^{m} \langle 0,1]) \in \llbracket\ g(d)\ \rrbracket^p$

Proof: By ⟨4⟩1

⟨4⟩3. $\{1\} \cap \sum_{j=1}^{m} \langle 0,1] = \{1\} \cap \langle 0,1] = \{1\}$

Proof: By Lemma 31

⟨4⟩4. Q.E.D.

Proof: By ⟨4⟩2 and ⟨4⟩3

⟨3⟩6. Q.E.D.

Proof: The cases ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4 and ⟨3⟩5 are exhaustive

$\langle 2\rangle 2.$ Q.E.D.
PROOF: Induction step

$\langle 1\rangle 3.$ Q.E.D.
PROOF: By induction with $\langle 1\rangle 1$ as base case and $\langle 1\rangle 2$ as induction step

□

**Lemma 37.** *Let $d \in \mathcal{D}^i$. Then*

$$\forall o \in [\![\ d\ ]\!]^i : \exists d' \in \mathcal{D}^u : [\![\ d'\ ]\!]^u = o$$

PROOF.

$\langle 1\rangle 1.$ CASE: $d = e$ for some event $e$ or $d = \mathsf{skip}$

$\langle 2\rangle 1.$ $d \in \mathcal{D}^u$
PROOF: By assumption $\langle 1\rangle 1$

$\langle 2\rangle 2.$ Q.E.D.
PROOF: By $\langle 2\rangle 1$; $d$ is the $d'$ we are looking for

$\langle 1\rangle 2.$ CASE: $d$ contains at least one operator

$\langle 2\rangle 1.$ ASSUME: For each operand $d_j$ occurring in an operand of $d$ the following holds: (ind. hyp.)
$\forall o_j \in [\![\ d_j\ ]\!]^i : \exists d'_j \in \mathcal{D}^u : [\![\ d'_j\ ]\!]^u = o_i$
PROVE: $\forall o \in [\![\ d\ ]\!]^i : \exists d' \in \mathcal{D}^u : [\![\ d'\ ]\!]^u = o$

$\langle 3\rangle 1.$ ASSUME: $o \in [\![\ d\ ]\!]^i$
PROVE: $\exists d' \in \mathcal{D}^u : [\![\ d'\ ]\!]^u = o$

$\langle 4\rangle 1.$ CASE: $d = \mathsf{refuse}\ d_1$

$\langle 5\rangle 1.$ LET: $(p_1, n_1) \in [\![\ d_1\ ]\!]^i$ s.t. $o = (\emptyset, p_1 \cup n_1)$
PROOF: By assumption $\langle 4\rangle 1$ and assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ LET: $d'_1 \in \mathcal{D}^u$ s.t. $[\![\ d'_1\ ]\!]^u = (p_1, n_1)$
PROOF: By $\langle 5\rangle 1$ and assumption $\langle 2\rangle 1$

$\langle 5\rangle 3.$ $[\![\ \mathsf{refuse}\ d'_1\ ]\!]^u = o$
PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

$\langle 5\rangle 4.$ $\mathsf{refuse}\ d'_1 \in \mathcal{D}^u$
PROOF: By $\langle 5\rangle 2$

$\langle 5\rangle 5.$ Q.E.D.
PROOF: By $\langle 5\rangle 3$ and $\langle 5\rangle 4$; $\mathsf{refuse}\ d'_1$ is the $d'$ we are looking for

$\langle 4\rangle 2.$ CASE: $d = d_1\ \mathsf{seq}\ d_2$

$\langle 5\rangle 1.$ LET: $o_1 \in [\![\ d_1\ ]\!]^i, o_2 \in [\![\ d_2\ ]\!]^i$ s.t. $o = o_1 \succsim o_2$
PROOF: By assumption $\langle 4\rangle 2$ and assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ LET: $d'_1, d'_2 \in \mathcal{D}^u$ s.t. $[\![\ d'_1\ ]\!]^u = o_1 \wedge [\![\ d'_2\ ]\!]^u = o_2$
PROOF: By $\langle 5\rangle 1$ and assumption $\langle 2\rangle 1$

$\langle 5\rangle 3.$ $[\![\ d'_1\ \mathsf{seq}\ d'_2\ ]\!]^u = o$
PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

$\langle 5\rangle 4.$ $d'_1\ \mathsf{seq}\ d'_2 \in \mathcal{D}^u$
PROOF: By $\langle 5\rangle 2$

$\langle 5\rangle 5.$ Q.E.D.
PROOF: By $\langle 5\rangle 3$ and $\langle 5\rangle 4$; $d'_1\ \mathsf{seq}\ d'_2$ is the $d'$ we are looking for

$\langle 4\rangle 3.$ CASE: $d = d_1\ \mathsf{par}\ d_2$

PROOF: Similar to ⟨4⟩3; replace $\mathsf{seq}$ with $\mathsf{par}$ and $\succsim$ with $\|$

⟨4⟩4. CASE: $d = d_1 \;\mathsf{alt}\; d_2$

PROOF: Similar to ⟨4⟩3; replace $\mathsf{seq}$ with $\mathsf{alt}$ and $\succsim$ with $\uplus$

⟨4⟩5. CASE: $d = d_1 \;\mathsf{xalt}\; d_2$

⟨5⟩1. $o \in \llbracket\, d_1 \,\rrbracket^i \vee o \in \llbracket\, d_2 \,\rrbracket^i$

PROOF: By assumption ⟨3⟩1 and assumption ⟨4⟩5

⟨5⟩2. CASE: $o \in \llbracket\, d_1 \,\rrbracket^i$

⟨6⟩1. LET: $d_1' \in \mathcal{D}^u$ s.t. $\llbracket\, d_1' \,\rrbracket^u = o$

PROOF: By assumption ⟨5⟩2 and assumption ⟨2⟩1

⟨6⟩2. Q.E.D.

PROOF: By ⟨6⟩1; $d_1'$ is the $d'$ we are looking for

⟨5⟩3. CASE: $o \in \llbracket\, d_2 \,\rrbracket^i$

PROOF: Similar to ⟨5⟩2

⟨5⟩4. Q.E.D.

PROOF: By ⟨5⟩1 the cases ⟨5⟩2 and ⟨5⟩3 are exhaustive

⟨4⟩6. Q.E.D.

PROOF: By assumption ⟨1⟩2 the cases ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 and ⟨4⟩5 are exhaustive

⟨3⟩2. Q.E.D.

PROOF: $\forall$-rule

⟨2⟩2. Q.E.D.

PROOF: Induction step

⟨1⟩3. Q.E.D.

PROOF: By induction with ⟨1⟩1 as base case and ⟨1⟩2 as induction step

□

**Lemma 38.**

$$d \in \mathcal{D}^i \Rightarrow \exists d' : N(d') \wedge \llbracket\, d \,\rrbracket^i = \llbracket\, d' \,\rrbracket^i$$

PROOF.

⟨1⟩1. ASSUME: $d \in \mathcal{D}^i$

PROVE: $\exists d' : N(d') \wedge \llbracket\, d \,\rrbracket^i = \llbracket\, d' \,\rrbracket^i$

⟨2⟩1. LET: $m \in \mathbb{N}$ s.t. $\#\llbracket\, d \,\rrbracket^i = m$

PROOF: By assumption ⟨1⟩1

⟨2⟩2. LET: $d_j \in \mathcal{D}^u$ s.t. $\llbracket\, d_j \,\rrbracket^u = o_j$ for each $o_j \in \llbracket\, d \,\rrbracket^i$

PROOF: By Lemma 37

⟨2⟩3. $\llbracket\, \mathsf{xalt}(d_1, \ldots, d_m) \,\rrbracket^i = \llbracket\, d \,\rrbracket^i$

PROOF: By ⟨2⟩2

⟨2⟩4. Q.E.D.

PROOF: By ⟨2⟩3 and ⟨2⟩2; $\llbracket\, \mathsf{xalt}(d_1, \ldots, d_m) \,\rrbracket^i$ is the $d'$ we are looking for

⟨1⟩2. Q.E.D.

PROOF: $\Rightarrow$-rule

□

**Lemma 39.** *Let $d \in \mathcal{D}^i$. Then*

$$(N(d) \wedge \exists s \subseteq \mathcal{H} : \forall (p,n) \in \llbracket\ d\ \rrbracket^i : p \cup n = s) \Rightarrow$$
$$\bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} p \cup n = \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} p \cup n \wedge$$
$$\bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} n = \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} n$$

Proof.

$\langle 1\rangle 1.$ Assume: 1. $N(d)$

2. $\exists s \subseteq \mathcal{H} : \forall (p,n) \in \llbracket\ d\ \rrbracket^i : p \cup n = s$

Prove: $\bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} p \cup n = \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} p \cup n \wedge$
$\bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} n = \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} n$

$\langle 2\rangle 1.$ Let: $s \subseteq \mathcal{H}$ s.t. $\forall (p,n) \in \llbracket\ d\ \rrbracket^i : p \cup n = s$

Proof: By assumption 2

$\langle 2\rangle 2.$ Let: $m \in \mathbb{N}$ s.t. $d = \mathsf{xalt}(d_1, \ldots, d_m)$

Proof: By assumption 1

$\langle 2\rangle 3.$ $\forall j \leq m : \#\llbracket\ d_j\ \rrbracket^i = 1$

Proof: $\langle 2\rangle 2$ and assumption 1

$\langle 2\rangle 4.$ $g(d) = \mathsf{palt}(d_1;\langle 0,1], \ldots, d_m;\langle 0,1])$

Proof: By $\langle 2\rangle 2$ and assumption 1 (which ensures that $g(d_j) = d_j$ for $1 \leq j \leq m$)

$\langle 2\rangle 5.$ $\bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} p \cup n = \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} p \cup n$

$\langle 3\rangle 1.$ $\bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} p \cup n \subseteq \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} p \cup n$

$\langle 4\rangle 1.$ Assume: $t \in \bigcap_{(p,n) \in \llbracket\ d\ \rrbracket^i} p \cup n$

Prove: $t \in \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} p \cup n$

$\langle 5\rangle 1.$ Assume: $t \notin \bigcap_{((p,n),Q) \in \llbracket\ g(d)\ \rrbracket^p} p \cup n$

Prove: $\perp$

$\langle 6\rangle 1.$ Let: $po' \in \llbracket\ g(d)\ \rrbracket^p$ s.t. $t \notin p' \cup n'$

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

$\langle 6\rangle 2.$ Case: $po' \in \{(\oplus \bigcup_{j \in N} \{po_j\}, \sum_{j \in N} Q_j) \mid N \subseteq \{1, \ldots, m\} \wedge N \neq \emptyset \wedge \forall j \in N : po_j \in \llbracket\ d_j;\langle 0,1]\ \rrbracket^p\}$

$\langle 7\rangle 1.$ Let: $N \subseteq \{1, \ldots, m\}$ s.t. $po' = (\oplus \bigcup_{j \in N} \{po_j\}, \sum_{j \in N} Q_j) \wedge N \neq \emptyset \wedge \forall j \in N : po_j \in \llbracket\ d_j;\langle 0,1]\ \rrbracket^p$

Proof: By assumption $\langle 6\rangle 2$

$\langle 7\rangle 2.$ $\bigcup_{j \in N} \{po_j\} = \bigcup_{j \in N} \llbracket\ d_j;\langle 0,1]\ \rrbracket^p$

Proof: By $\langle 7\rangle 1$ and $\langle 2\rangle 3$

$\langle 7\rangle 3.$ $o' = \oplus \bigcup_{j \in N} \llbracket\ d_j;\langle 0,1]\ \rrbracket^p$

Proof: By ⟨7⟩2 and ⟨7⟩1

⟨7⟩4. $\bigcup_{j \in N} [\![\ d_j\ ]\!]^i \subseteq [\![\ d\ ]\!]^i$

Proof: By ⟨2⟩2 and ⟨7⟩1 ($N \subseteq \{1, \ldots, m\}$)

⟨7⟩5. $\forall po \in \bigcup_{j \in N} [\![\ d_j;\langle 0,1]\ ]\!]^p : t \in p \cup n$

Proof: By ⟨7⟩4 and assumption ⟨4⟩1

⟨7⟩6. $t \in p' \cup n'$

Proof: By ⟨7⟩5 and ⟨7⟩3

⟨7⟩7. Q.E.D.

Proof: By ⟨7⟩6 and ⟨6⟩1

⟨6⟩3. Case: $po' = (\oplus \bigcup_{j=1}^{m} [\![\ d_j;\langle 0,1]\ ]\!]^p, \{1\} \cap \sum_{j=1}^{m} \langle 0,1])$

⟨7⟩1. Let: $k \leq m$ s.t. $[\![\ d_k\ ]\!]^i = \{(p_k, n_k)\} \wedge t \notin p_k \cup n_k$

Proof: By assumption ⟨6⟩3, assumption ⟨6⟩1 and ⟨2⟩3

⟨7⟩2. $(p_k, n_k) \in [\![\ d\ ]\!]^i$

Proof: By ⟨7⟩1 and ⟨2⟩2

⟨7⟩3. $t \in p_k \cup n_k$

Proof: By ⟨7⟩2 and ⟨4⟩1

⟨7⟩4. Q.E.D.

Proof: By ⟨7⟩1 and ⟨7⟩3

⟨6⟩4. Q.E.D.

Proof: By ⟨6⟩1 ($po \in [\![\ g(d)\ ]\!]^p$) and ⟨2⟩4 the cases ⟨6⟩2 and ⟨6⟩3 are exhaustive

⟨5⟩2. Q.E.D.

Proof: ⊥-rule

⟨4⟩2. Q.E.D.

Proof: ⊆-rule

⟨3⟩2. $\bigcap_{((p,n),Q) \in [\![\ g(d)\ ]\!]^p} p \cup n \subseteq \bigcap_{(p,n) \in [\![\ d\ ]\!]^i} p \cup n$

⟨4⟩1. Assume: $t \in \bigcap_{((p,n),Q) \in [\![\ g(d)\ ]\!]^p} p \cup n$

Prove: $t \in \bigcap_{(p,n) \in [\![\ d\ ]\!]^i} p \cup n$

⟨5⟩1. $\forall ((p,n),Q) \in [\![\ g(d)\ ]\!]^p : t \in p \cup n$

Proof: By assumption ⟨4⟩1

⟨5⟩2. $\forall (p,n) \in [\![\ g(d)\ ]\!]^i : t \in p \cup n$

Proof: By ⟨5⟩1 and Lemma 34

⟨5⟩3. Q.E.D.

Proof: By ⟨5⟩2

⟨4⟩2. Q.E.D.

Proof: ⊆-rule

⟨3⟩3. Q.E.D.

Proof: By ⟨3⟩1 and ⟨3⟩2

⟨2⟩6. $\bigcap_{(p,n) \in [\![\ d\ ]\!]^i} n = \bigcap_{((p,n),Q) \in [\![\ g(d)\ ]\!]^p} n$

⟨3⟩1. $\bigcap_{(p,n)\in[\![\ d\ ]\!]^i} n \subseteq \bigcap_{((p,n),Q)\in[\![\ g(d)\ ]\!]^p} n$

⟨4⟩1. ASSUME: $t \in \bigcap_{(p,n)\in[\![\ d\ ]\!]^i} n$

PROVE: $t \in \bigcap_{((p,n),Q)\in[\![\ g(d)\ ]\!]^p} n$

⟨5⟩1. ASSUME: $t \notin \bigcap_{((p,n),Q)\in[\![\ g(d)\ ]\!]^p} n$

PROVE: $\perp$

⟨6⟩1. LET: $po' \in [\![\ g(d)\ ]\!]^p$ s.t. $t \notin n'$

PROOF: By assumption ⟨5⟩1

⟨6⟩2. CASE: $po' \in \{(\oplus \bigcup_{j\in N}\{po_j\}, \sum_{j\in N} Q_j) \mid N \subseteq \{1,\ldots,m\} \wedge N \neq \emptyset \wedge \forall j \in N : po_j \in [\![\ d_j;\langle 0,1]\ ]\!]^p\}$

⟨7⟩1. LET: $N \subseteq \{1,\ldots,m\}$ s.t. $po' = (\oplus \bigcup_{j\in N}\{po_j\}, \sum_{j\in N} Q_j) \wedge N \neq \emptyset \wedge \forall j \in N : po_j \in [\![\ d_j;\langle 0,1]\ ]\!]^p$

PROOF: By assumption ⟨6⟩2

⟨7⟩2. $\bigcup_{j\in N}\{po_j\} = \bigcup_{j\in N} [\![\ d_j;\langle 0,1]\ ]\!]^p$

PROOF: By ⟨7⟩1 and ⟨2⟩3

⟨7⟩3. $o' = \oplus \bigcup_{j\in N} [\![\ d_j;\langle 0,1]\ ]\!]^p$

PROOF: By ⟨7⟩2 and ⟨7⟩1

⟨7⟩4. $\bigcup_{j\in N} [\![\ d_j\ ]\!]^i \subseteq [\![\ d\ ]\!]^i$

PROOF: By ⟨2⟩2 and ⟨7⟩1 ($N \subseteq \{1,\ldots,m\}$)

⟨7⟩5. $\forall po \in \bigcup_{j\in N} [\![\ d_j;\langle 0,1]\ ]\!]^p : t \in n$

PROOF: By ⟨7⟩4 and assumption ⟨4⟩1

⟨7⟩6. $t \in n'$

PROOF: By ⟨7⟩5 and ⟨7⟩3

⟨7⟩7. Q.E.D.

PROOF: By ⟨7⟩6 and ⟨6⟩1

⟨6⟩3. CASE: $po' = (\oplus \bigcup_{j=1}^{m} [\![\ d_j;\langle 0,1]\ ]\!]^p, \{1\} \cap \sum_{j=1}^{m} \langle 0,1])$

⟨7⟩1. LET: $k \leq m$ s.t. $[\![\ d_k\ ]\!]^i = \{(p_k,n_k)\} \wedge t \notin n_k$

PROOF: By assumption ⟨6⟩3, assumption ⟨6⟩1 and ⟨2⟩3

⟨7⟩2. $(p_k,n_k) \in [\![\ d\ ]\!]^i$

PROOF: By ⟨7⟩1 and ⟨2⟩2

⟨7⟩3. $t \in n_k$

PROOF: By ⟨7⟩2 and ⟨4⟩1

⟨7⟩4. Q.E.D.

PROOF: By ⟨7⟩1 and ⟨7⟩3

⟨6⟩4. Q.E.D.

PROOF: By ⟨6⟩1 ($po \in [\![\ g(d)\ ]\!]^p$) and ⟨2⟩4 the cases ⟨6⟩2 and ⟨6⟩3 are exhaustive

⟨5⟩2. Q.E.D.

PROOF: $\perp$-rule

⟨4⟩2. Q.E.D.
PROOF: ⊆-rule

⟨3⟩2. $\bigcap_{((p,n),Q)\in[\![\ g(d)\ ]\!]^p} n \subseteq \bigcap_{(p,n)\in[\![\ d\ ]\!]^i} n$

⟨4⟩1. ASSUME: $t \in \bigcap_{((p,n),Q)\in[\![\ g(d)\ ]\!]^p} n$
PROVE: $t \in \bigcap_{(p,n)\in[\![\ d\ ]\!]^i} n$

⟨5⟩1. $\forall((p,n),Q) \in [\![\ g(d)\ ]\!]^p : t \in n$
PROOF: By assumption ⟨4⟩1

⟨5⟩2. $\forall(p,n) \in [\![\ g(d)\ ]\!]^i : t \in n$
PROOF: By ⟨5⟩1 and Lemma 34

⟨5⟩3. Q.E.D.
PROOF: By ⟨5⟩2

⟨4⟩2. Q.E.D.
PROOF: ⊆-rule

⟨3⟩3. Q.E.D.
PROOF: By ⟨3⟩1 and ⟨3⟩2

⟨2⟩7. Q.E.D.
PROOF: By ⟨2⟩5 and ⟨2⟩6

⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

**Lemma 40.** *Let $O_1$, $O_2$, $O_1'$ and $O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{pl} O_1' \wedge O_2 \rightsquigarrow_{pl} O_2' \Rightarrow \oplus(O_1 \succsim O_2) \rightsquigarrow_r \oplus(O_1' \succsim O_2')$$

PROOF.

⟨1⟩1. ASSUME: $O_1 \rightsquigarrow_{pl} O_1' \wedge O_2 \rightsquigarrow_{pl} O_2'$
PROVE: $\oplus(O_1 \succsim O_2) \rightsquigarrow_r \oplus(O_1' \succsim O_2')$

⟨2⟩1. LET: $(p_3, n_3) = \oplus(O_1 \succsim O_2)$
$(p_4, n_4) = \oplus(O_1' \succsim O_2')$

⟨2⟩2. ASSUME: $(p_3, n_3) \not\rightsquigarrow_r (p_4, n_4)$
PROVE: $\bot$

⟨3⟩1. $n_3 \not\subseteq n_4 \vee p_3 \not\subseteq p_4 \cup n_4$
PROOF: By assumption ⟨2⟩2

⟨3⟩2. CASE: $n_3 \not\subseteq n_4$

⟨4⟩1. LET: $t \in \mathcal{H}$ such that $t \in n_3 \wedge t \notin n_4$
PROOF: By assumption ⟨3⟩2

⟨4⟩2. $\forall po \in O_1 \succsim O_2 : t \in n$
PROOF: By ⟨4⟩1

⟨4⟩3. $\forall po_1 \in O_1, po_2 \in O_2 : t \in (n_1 \succsim p_2) \cup (n_1 \succsim n_2) \cup (p_1 \succsim n_2)$
PROOF: By ⟨4⟩2

⟨4⟩4. $\exists po \in O_1' \succsim O_2' : t \notin n$
PROOF: By ⟨4⟩1

⟨4⟩5. Let: $po_1' \in O_1', po_2' \in O_2'$ such that $t \notin (n_1' \succsim p_2') \cup (n_1' \succsim n_2') \cup (p_1' \succsim n_2')$

Proof: By ⟨4⟩4

⟨4⟩6. $\forall S_1 \subseteq O_1', S_2 \subseteq O_2' : po_1' \in S_1 \wedge po_2' \in S_2 \Rightarrow t \notin \pi_2.\oplus(S_1 \succsim S_2)$

Proof: By ⟨4⟩5 and definition 4

⟨4⟩7. Let: $S_1 \subseteq O_1', po_1 \in O_1$ such that $po_1' \in S_1 \wedge po_1 \rightsquigarrow_{pr} \bar{\oplus} S_1$
$S_2 \subseteq O_2', po_2 \in O_2$ such that $po_2' \in S_2 \wedge po_2 \rightsquigarrow_{pr} \bar{\oplus} S_2$

Proof: By assumption ⟨1⟩1

⟨4⟩8. $t \in (n_1 \succsim p_2) \cup (n_1 \succsim n_2) \cup (p_1 \succsim n_2)$

Proof: By ⟨4⟩7 and ⟨4⟩3

⟨4⟩9. Case: $t \in n_1 \succsim p_2$

⟨5⟩1. Let: $t_1 \in n_1, t_2 \in p_2$ such that $t \in \{t_1\} \succsim \{t_2\}$

Proof: By assumption ⟨4⟩9

⟨5⟩2. $\forall po \in S_1 : t_1 \in n$

Proof: By ⟨5⟩1 and ⟨4⟩7 ($po_1 \rightsquigarrow_{pr} \bar{\oplus} S_1$)

⟨5⟩3. $\forall po \in S_2 : t_2 \in p \cup n$

Proof: By ⟨5⟩1 and ⟨4⟩7 ($po_2 \rightsquigarrow_{pr} \bar{\oplus} S_2$)

⟨5⟩4. $\forall po \in S_1 \succsim S_2 : t \in n$

Proof: By ⟨5⟩2, ⟨5⟩3 and ⟨5⟩1 ($t \in \{t_1\} \succsim \{t_2\}$)

⟨5⟩5. $t \in \pi_2.\oplus(S_1 \succsim S_2)$

Proof: By ⟨5⟩4

⟨5⟩6. Q.E.D.

Proof: By ⟨5⟩5, ⟨4⟩6 and ⟨4⟩7 ($po_1' \in S_1, po_2' \in S_2$)

⟨4⟩10. Case: $t \in n_1 \succsim n_2$

⟨5⟩1. Let: $t_1 \in n_1, t_2 \in n_2$ such that $t \in \{t_1\} \succsim \{t_2\}$

Proof: By assumption ⟨4⟩10

⟨5⟩2. $\forall po \in S_1 : t_1 \in n$

Proof: By ⟨5⟩1 and ⟨4⟩7 ($po_1 \rightsquigarrow_{pr} \bar{\oplus} S_1$)

⟨5⟩3. $\forall po \in S_2 : t_2 \in n$

Proof: By ⟨5⟩1 and ⟨4⟩7 ($po_2 \rightsquigarrow_{pr} \bar{\oplus} S_2$)

⟨5⟩4. $\forall po \in S_1 \succsim S_2 : t \in n$

Proof: By ⟨5⟩2, ⟨5⟩3 and ⟨5⟩1 ($t \in \{t_1\} \succsim \{t_2\}$)

⟨5⟩5. $t \in \pi_2.\oplus(S_1 \succsim S_2)$

Proof: By ⟨5⟩4

⟨5⟩6. Q.E.D.

Proof: By ⟨5⟩5 and ⟨4⟩6 and ⟨4⟩7 ($po_1' \in S_1, po_2' \in S_2$)

⟨4⟩11. Case: $t \in p_1 \succsim n_2$

Proof: Similar to case ⟨4⟩9

⟨4⟩12. Q.E.D.

Proof: By ⟨4⟩8 the cases ⟨4⟩9, ⟨4⟩10 and ⟨4⟩11 are exhaustive

⟨3⟩3. Case: $p_3 \nsubseteq p_4 \cup n_4$

⟨4⟩1. Let: $t \in \mathcal{H}$ such that $t \in p_3 \wedge t \notin p_4 \cup n_4$

Proof: By assumption ⟨3⟩3

⟨4⟩2. $\forall po \in O_1 \succsim O_2 : t \in p \cup n$

Proof: By ⟨4⟩1

⟨4⟩3. $\forall po_1 \in O_1, po_2 \in O_2 : t \in (p_1 \succsim p_2) \cup (n_1 \succsim p_2) \cup (n_1 \succsim n_2) \cup (p_1 \succsim n_2)$

PROOF: By ⟨4⟩2

⟨4⟩4. $\exists po \in O_1' \succsim O_2' : t \notin p \cup n$

PROOF: By ⟨4⟩1

⟨4⟩5. LET: $po_1' \in O_1', po_2' \in O_2'$ such that $t \notin (p_1' \succsim p_2') \cup (n_1' \succsim p_2') \cup (n_1' \succsim n_2') \cup (p_1' \succsim n_2')$

PROOF: By ⟨4⟩4

⟨4⟩6. $\forall S_1 \subseteq O_1', S_2' \subseteq O_2' : po_1' \in S_1 \wedge po_2' \in S_2 \Rightarrow t \notin \pi_1.\oplus(S_1 \succsim S_2) \cup \pi_2.\oplus(S_1 \succsim S_2)$

PROOF: By ⟨4⟩5 and definition 4

⟨4⟩7. LET: $S_1 \subseteq O_1', po_1 \in O_1$ such that $po_1' \in S_1 \wedge po_1 \rightsquigarrow_r \bar{\oplus} S_1$
$S_2 \subseteq O_2', po_2 \in O_2$ such that $po_2' \in S_2 \wedge po_2 \rightsquigarrow_r \bar{\oplus} S_2$

PROOF: By assumption ⟨1⟩1 and ⟨4⟩5

⟨4⟩8. $t \in (p_1 \succsim p_2) \cup (n_1 \succsim p_2) \cup (n_1 \succsim n_2) \cup (p_1 \succsim n_2)$

PROOF: By ⟨4⟩3 and ⟨4⟩7

⟨4⟩9. CASE: $t \in p_1 \succsim p_2$

⟨5⟩1. LET: $t_1 \in p_1, t_2 \in p_2$ such that $t \in \{t_1\} \succsim \{t_2\}$

PROOF: By assumption ⟨4⟩9

⟨5⟩2. $\forall po \in S_1 : t_1 \in p \cup n$

PROOF: By ⟨5⟩1 and ⟨4⟩7 ($po_1 \rightsquigarrow_{pr} \bar{\oplus} S_1$)

⟨5⟩3. $\forall po \in S_2 : t_2 \in p \cup n$

PROOF: By ⟨5⟩1 and ⟨4⟩7 ($po_2 \rightsquigarrow_{pr} \bar{\oplus} S_2$)

⟨5⟩4. $\forall po \in S_1 \succsim S_2 : t \in p \cup n$

PROOF: By ⟨5⟩2, ⟨5⟩3 and ⟨5⟩1 ($t \in \{t_1\} \succsim \{t_2\}$)

⟨5⟩5. $t \in \pi_1.\oplus(S_1 \succsim S_2) \cup \pi_2.\oplus(S_1 \succsim S_2)$

PROOF: By ⟨5⟩4 and definition 4

⟨5⟩6. Q.E.D.

PROOF: By ⟨5⟩5, ⟨4⟩6 and ⟨4⟩5 ($po_1' \in S_1, po_2' \in S_2$)

⟨4⟩10. CASE: $t \in n_1 \succsim p_2$

PROOF: Similar to case ⟨4⟩9

⟨4⟩11. CASE: $t \in n_1 \succsim n_2$

PROOF: Similar to case ⟨4⟩9

⟨4⟩12. CASE: $t \in p_1 \succsim n_2$

PROOF: Similar to case ⟨4⟩9

⟨4⟩13. Q.E.D.

PROOF: By ⟨4⟩8 the cases ⟨4⟩9, ⟨4⟩10, ⟨4⟩11 and ⟨4⟩12 are exhaustive

⟨3⟩4. Q.E.D.

PROOF: By ⟨3⟩1 the cases ⟨3⟩2 and ⟨3⟩3 are exhaustive

⟨2⟩3. Q.E.D.

PROOF: ⊥-rule

⟨1⟩2. Q.E.D.

PROOF: ⇒-rule

□

**Lemma 41.** *Let $O_1$, $O_2$, $O_1'$ and $O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{pl} O_1' \wedge O_2 \rightsquigarrow_{pl} O_2' \Rightarrow \oplus(O_1 \parallel O_2) \rightsquigarrow_{r} \oplus(O_1' \parallel O_2')$$

Proof. The proof is similar to the proof for Lemma 40; just replace $\succsim$ with $\parallel$. □

**Lemma 42.** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\begin{aligned}\llbracket d_1 \rrbracket \rightsquigarrow_{pg} \llbracket d_1' \rrbracket \wedge \llbracket d_2 \rrbracket \rightsquigarrow_{pg} \llbracket d_2' \rrbracket \Rightarrow\ & \pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket)) \ \wedge \\ & \pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ par\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ par\ } d_2 \rrbracket)) \ \wedge \\ & \pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ alt\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ alt\ } d_2 \rrbracket))\end{aligned}$$

Proof.

⟨1⟩1. Assume: $\llbracket d_1 \rrbracket \rightsquigarrow_{pg} \llbracket d_1' \rrbracket \wedge \llbracket d_2 \rrbracket \rightsquigarrow_{pg} \llbracket d_2' \rrbracket$
Prove: $\pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket))\wedge$
$\pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ par\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ par\ } d_2 \rrbracket))\wedge$
$\pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ alt\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ alt\ } d_2 \rrbracket))$

⟨2⟩1. $\pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket))$

⟨3⟩1. $\pi_2.\bar{\oplus}\llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket \subseteq \{1\}$
Proof: By Lemma 2

⟨3⟩2. $1 \in \pi_2.\bar{\oplus}\llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket \Rightarrow 1 \in \pi_2.\bar{\oplus}\llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket$

⟨4⟩1. Assume: $1 \in \pi_2.\bar{\oplus}\llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket$
Prove: $1 \in \pi_2.\bar{\oplus}\llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket$

⟨5⟩1. $\forall po \in \llbracket d_1' \mathsf{\ seq\ } d_2' \rrbracket : \pi_2.po \neq \emptyset$
Proof: By assumption ⟨4⟩1

⟨5⟩2. $\forall po \in \llbracket d_1' \rrbracket \cup \llbracket d_2' \rrbracket : \pi_2.po \neq \emptyset$
Proof: By ⟨5⟩1

⟨5⟩3. $\forall po \in \llbracket d_1 \rrbracket \cup \llbracket d_2 \rrbracket : \pi_2.po \neq \emptyset$
Proof: By ⟨5⟩2 and assumption ⟨1⟩1 (since each p-obligation in $\llbracket d_1 \rrbracket$ either has 0 in its probability set or is represented in $\llbracket d_1' \rrbracket$, and each p-obligation in $\llbracket d_2 \rrbracket$ either has 0 in its probability set or is represented in $\llbracket d_2' \rrbracket$)

⟨5⟩4. $\forall po \in \llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket : \pi_2.po \neq \emptyset$
Proof: By ⟨5⟩3

⟨5⟩5. $\pi_2.\bar{\oplus}\llbracket d_1 \mathsf{\ seq\ } d_2 \rrbracket \neq \emptyset$
Proof: By ⟨5⟩4

⟨5⟩6. Q.E.D.
Proof: By ⟨5⟩5 and Lemma 2

⟨4⟩2. Q.E.D.
Proof: $\Rightarrow$-rule

⟨3⟩3. Q.E.D.
Proof: By ⟨3⟩1 and ⟨3⟩2

⟨2⟩2. $\pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ par\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ par\ } d_2 \rrbracket))$
Proof: Similar to ⟨2⟩1; just replace seq with par.

⟨2⟩3. $\pi_2(\bar{\oplus}(\llbracket d_1' \mathsf{\ alt\ } d_2' \rrbracket)) \subseteq \pi_2(\bar{\oplus}(\llbracket d_1 \mathsf{\ alt\ } d_2 \rrbracket))$

Proof: Similar to $\langle 2\rangle 1$; just replace seq with alt.

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

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

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

Proof: $\Rightarrow$-rule

□

**Lemma 43.**

$$E(d) \Rightarrow \exists s \in \mathcal{H} : \forall((p,n),Q) \in [\![\ g(d)\ ]\!]^p : p \cup n = s$$

Proof.

$\langle 1\rangle 1.$ Assume: $E(d)$

Prove: $\exists s \subseteq \mathcal{H} : \forall((p,n),Q) \in [\![\ g(d)\ ]\!]^p : p \cup n = s$

$\langle 2\rangle 1.$ Case: $d$ consists of a single event $e$ or $d = \mathsf{skip}$

$\langle 3\rangle 1.$ $d$ consists of a single event $e$

$\langle 4\rangle 1.$ $[\![\ g(d)\ ]\!]^p = \{((\{\langle e\rangle\}, \emptyset), \{1\})\}$

Proof: By assumption $\langle 2\rangle 1$

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

Proof: By $\langle 3\rangle 1$; $\{\langle e\rangle\}$ is the $s$ we are looking for

$\langle 3\rangle 2.$ $d = \mathsf{skip}$

Proof: Similar to $\langle 3\rangle 1$; just replace $\langle e\rangle$ with $\langle\rangle$

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

Proof: By assumption $\langle 2\rangle 1$ the cases $\langle 3\rangle 1$ and $\langle 3\rangle 2$ are exhaustive

$\langle 2\rangle 2.$ Case: $d$ contains at least one operator

$\langle 3\rangle 1.$ Assume: For every sequence diagram $d'$ that occurs in an operand of $d$ the following holds:
$\exists s' \subseteq \mathcal{H} : \forall((p',n'),Q') \in [\![\ g(d')\ ]\!] : p' \cup n' = s'$ (ind. hyp.)

Prove: $\exists s \subseteq \mathcal{H} : \forall((p,n),Q) \in [\![\ g(d)\ ]\!] : p \cup n = s$

$\langle 4\rangle 1.$ Case: $d = \mathsf{refuse}\ d_1$

$\langle 5\rangle 1.$ $g(d) = \mathsf{refuse}\ g(d_1)$

Proof: By assumption $\langle 4\rangle 1$

$\langle 5\rangle 2.$ Let: $s_1 \subseteq \mathcal{H}$ s.t. $\forall((p_1,n_1),Q_1) \in [\![\ g(d_1)\ ]\!] : p_1 \cup n_1 = s_1$

Proof: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 3.$ $\forall((p,n),Q) \in [\![\ g(d)\ ]\!]^p : p = \emptyset \wedge n = s_1$

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 1$

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

Proof: By $\langle 5\rangle 3$; $s_1$ is the $s$ we are looking for

$\langle 4\rangle 2.$ Case: $d = d_1\ \mathsf{seq}\ d_2$

$\langle 5\rangle 1.$ $g(d) = g(d_1)\ \mathsf{seq}\ g(d_2)$

Proof: By assumption $\langle 4\rangle 2$

$\langle 5\rangle 2.$ Let: $s_1 \subseteq \mathcal{H}$ s.t. $\forall((p_1,n_1),Q_1) \in [\![\ g(d_1)\ ]\!]^p : p_1 \cup n_1 = s_1$
$s_2 \subseteq \mathcal{H}$ s.t. $\forall((p_2,n_2),Q_2) \in [\![\ g(d_2)\ ]\!]^p : p_2 \cup n_2 = s_2$

Proof: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 3.$ $\forall po \in [\![\ g(d)\ ]\!]^p : p \cup n = s_1 \succsim s_2$

$\langle 6\rangle 1.$ Assume: $po' \in [\![\ g(d)\ ]\!]^p$

Prove: $p' \cup n' = s_1 \succsim s_2$

⟨7⟩1. Let: $po_1 \in [\![\ g(d_1)\ ]\!]^p, po_2 \in [\![\ g(d_2)\ ]\!]^p$ s.t. $po' = po_1 \succsim po_2$

Proof: By assumption ⟨6⟩1 and ⟨5⟩1

⟨7⟩2. $p_1 \cup n_1 = s_1 \wedge p_2 \cup n_2 = s_2$

Proof: By ⟨7⟩1 and ⟨5⟩2

⟨7⟩3. $p' \cup n' = (p_1 \succsim p_2) \cup (p_1 \succsim n_2) \cup (n_1 \succsim p_2) \cup (n_1 \succsim n_2)$

Proof: By ⟨7⟩1

⟨7⟩4. $(p_1 \succsim p_2) \cup (p_1 \succsim n_2) \cup (n_1 \succsim p_2) \cup (n_1 \succsim n_2) = s_1 \succsim s_2$

Proof: $(p_1 \succsim p_2) \cup (p_1 \succsim n_2) \cup (n_1 \succsim p_2) \cup (n_1 \succsim n_2)$

$= (p_1 \succsim (p_2 \cup n_2)) \cup (n_1 \succsim (p_2 \cup n_2))$

By Lemma 14 in [HHRS06]

$= (p_1 \cup n_1) \succsim (p_2 \cup n_2)$

By Lemma 15 in [HHRS06]

$= s_1 \succsim s_2$

By ⟨7⟩2

⟨7⟩5. Q.E.D.

Proof: By ⟨7⟩3 and ⟨7⟩4

⟨6⟩2. Q.E.D.

Proof: $\forall$-rule

⟨5⟩4. Q.E.D.

Proof: By ⟨5⟩3; $s_1 \succsim s_2$ is the $s$ we are looking for

⟨4⟩3. Case: $d = d_1$ par $d_2$

Proof: Similar to case ⟨4⟩2; just replace the references to Lemma 14 and Lemma 15 in [HHRS06] with references to Lemma 12 and Lemma 13 in [HHRS06]

⟨4⟩4. Case: $d = d_1$ alt $d_2$

⟨5⟩1. $g(d) = g(d_1)$ alt $g(d_2)$

Proof: By assumption ⟨4⟩4

⟨5⟩2. Let: $s_1 \subseteq \mathcal{H}$ s.t. $\forall((p_1, n_1), Q_1) \in [\![\ g(d_1)\ ]\!]^p : p_1 \cup n_1 = s_1$
$s_2 \subseteq \mathcal{H}$ s.t. $\forall((p_2, n_2), Q_2) \in [\![\ g(d_2)\ ]\!]^p : p_2 \cup n_2 = s_2$

Proof: By assumption ⟨3⟩1

⟨5⟩3. $\forall((p, n), Q) \in [\![\ g(d)\ ]\!]^p : p \cup n = s_1 \cup s_2$

⟨6⟩1. Assume: $po' \in [\![\ g(d)\ ]\!]^p$
Prove: $p' \cup n' = s_1 \cup s_2$

⟨7⟩1. Let: $po_1 \in [\![\ g(d_1)\ ]\!]^p, po_2 \in [\![\ g(d_2)\ ]\!]^p$ s.t. $po' = po_1 \uplus po_2$

Proof: By assumption ⟨6⟩1 and ⟨5⟩1

⟨7⟩2. $p_1 \cup n_1 = s_1 \wedge p_2 \cup n_2 = s_2$

Proof: By ⟨7⟩1 and ⟨5⟩2

⟨7⟩3. $p' \cup n' = (p_1 \cup p_2) \cup (n_1 \cup n_2)$

Proof: By ⟨7⟩2 and ⟨7⟩1

⟨7⟩4. $(p_1 \cup p_2) \cup (n_1 \cup n_2) = s_1 \cup s_2$

Proof: By ⟨7⟩2

⟨7⟩5. Q.E.D.

Proof: By ⟨7⟩3 and ⟨7⟩4

⟨6⟩2. Q.E.D.

PROOF: $\forall$-rule

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

PROOF: By $\langle 5\rangle 3$; $s_1 \cup s_2$ is the $s$ we are looking for

$\langle 4\rangle 5$. CASE: $d = \mathsf{xalt}(d_1, \ldots, d_n)$

$\langle 5\rangle 1$. $g(d) = \mathsf{palt}(g(d_1);\langle 0,1], \ldots, g(d_n);\langle 0,1])$

PROOF: By assumption $\langle 4\rangle 5$

$\langle 5\rangle 2$. LET: $s' \subseteq \mathcal{H}$ s.t. $\forall o \in \bigcup_{j\in\{1,\ldots,n\}} [\![\ d_j\ ]\!]^i : p \cup n = s'$

PROOF: By assumption $\langle 1\rangle 1$ and assumption $\langle 4\rangle 5$

$\langle 5\rangle 3$. $\forall po \in [\![\ g(d)\ ]\!]^p : p \cup n = s'$

$\langle 6\rangle 1$. ASSUME: $po' \in [\![\ g(d)\ ]\!]^p$

PROVE: $p' \cup n' = s'$

$\langle 7\rangle 1$. $\forall j \in \{1, \ldots, n\} : \forall po \in [\![\ g(d_j)\ ]\!]^p : p \cup n = s'$

$\langle 8\rangle 1$. ASSUME: $j \in \{1, \ldots, n\}$

PROVE: $\forall po \in [\![\ g(d_j)\ ]\!]^p : p \cup n = s'$

$\langle 9\rangle 1$. LET: $s_j \subseteq \mathcal{H}$ s.t. $\forall po \in [\![\ g(d_j)\ ]\!]^p : p \cup n = s_j$

PROOF: By assumption $\langle 3\rangle 1$

$\langle 9\rangle 2$. $s_j = s'$

$\langle 10\rangle 1$. LET: $o_j \in [\![\ d_j\ ]\!]^i$

$\langle 10\rangle 2$. LET: $Q_j \subseteq [0,1]$ s.t. $(o_j, Q_j) \in [\![\ g(d_j)\ ]\!]^p$

PROOF: By $\langle 10\rangle 1$ and Lemma 34

$\langle 10\rangle 3$. $p_j \cup n_j = s_j$

PROOF: By $\langle 10\rangle 2$ and $\langle 9\rangle 1$

$\langle 10\rangle 4$. $p_j \cup n_j = s'$

PROOF: By $\langle 10\rangle 1$ and $\langle 5\rangle 2$

$\langle 10\rangle 5$. Q.E.D.

PROOF: By $\langle 10\rangle 3$ and $\langle 10\rangle 4$

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

PROOF: By $\langle 9\rangle 1$ and $\langle 9\rangle 2$

$\langle 8\rangle 2$. Q.E.D.

PROOF: $\forall$-rule

$\langle 7\rangle 2$. LET: $S \subseteq \bigcup_{j\in\{1,\ldots,n\}} [\![\ g(d_j)\ ]\!]^p$ s.t. $o' = \oplus S$

PROOF: By assumption $\langle 6\rangle 1$ and $\langle 5\rangle 1$

$\langle 7\rangle 3$. $\forall po \in S : p \cup n = s'$

PROOF: By $\langle 7\rangle 2$ ($S \subseteq \bigcup_{j\in\{1,\ldots,n\}} [\![\ g(d_j)\ ]\!]^p$) and $\langle 7\rangle 1$

$\langle 7\rangle 4$. Q.E.D.

PROOF: By $\langle 7\rangle 3$ and $\langle 7\rangle 2$

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

PROOF: $\forall$-rule

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

PROOF: By $\langle 5\rangle 3$; $s'$ is the $s$ we are looking for

$\langle 4\rangle 6$. Q.E.D.

PROOF: By assumption $\langle 2\rangle 2$, the cases $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$ and $\langle 4\rangle 5$ are exhaustive

⟨3⟩2. Q.E.D.
PROOF: Induction step
⟨2⟩3. Q.E.D.
PROOF: Induction with ⟨2⟩1 as basis and ⟨2⟩2 as induction step
⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

**Lemma 44.**

$$E(d) \Rightarrow \forall (o, Q) \in [\![\ g(d)\ ]\!]^p : \exists o' \in [\![\ d\ ]\!]^i : o \rightsquigarrow_{nr} o'$$

PROOF.

⟨1⟩1. ASSUME: $E(d)$
PROVE: $\forall (o, Q) \in [\![\ g(d)\ ]\!]^p : \exists o' \in [\![\ d\ ]\!]^i : o \rightsquigarrow_{nr} o'$
⟨2⟩1. ASSUME: $(o_1, Q_1) \in [\![\ g(d)\ ]\!]^p$
PROVE: $\exists o' \in [\![\ d\ ]\!]^i : o_1 \rightsquigarrow_{nr} o'$
⟨3⟩1. LET: $s \subseteq \mathcal{H}$ s.t. $\forall po \in [\![\ g(d)\ ]\!]^p : p \cup n = s$
PROOF: By assumption ⟨1⟩1 and Lemma 43
⟨3⟩2. LET: $o_2 \in [\![\ d\ ]\!]^i$ s.t. $o_1 \rightsquigarrow_r o_2$
PROOF: By assumption ⟨2⟩1 and Lemma 35
⟨3⟩3. $o_1 \rightsquigarrow_{nr} o_2$
⟨4⟩1. $p_1 \cup n_1 = p_2 \cup n_2$
⟨5⟩1. $p_1 \cup n_1 = s$
PROOF: By assumption ⟨2⟩1 and ⟨3⟩1
⟨5⟩2. $p_2 \cup n_2 = s$
PROOF: By ⟨3⟩2, ⟨3⟩1 and Lemma 34
⟨5⟩3. Q.E.D.
PROOF: By ⟨5⟩1 and ⟨5⟩2
⟨4⟩2. Q.E.D.
PROOF: By ⟨4⟩1 and ⟨3⟩2
⟨3⟩4. Q.E.D.
PROOF: By ⟨3⟩2 and ⟨3⟩3; $o_2$ is the $o'$ we are looking for
⟨2⟩2. Q.E.D.
PROOF: ∀-rule
⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

### Transitivity

**Theorem 11 (Transitivity of $\rightsquigarrow_{prg}$).** *Let $d$, $d'$ and $d''$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d\ ]\!] \rightsquigarrow_{prg} [\![\ d'\ ]\!] \wedge [\![\ d'\ ]\!] \rightsquigarrow_{prg} [\![\ d''\ ]\!] \Rightarrow [\![\ d\ ]\!] \rightsquigarrow_{prg} [\![\ d''\ ]\!]$$

Proof.

⟨1⟩1. Assume: $\llbracket\, d \,\rrbracket \rightsquigarrow_{prg} \llbracket\, d' \,\rrbracket \wedge \llbracket\, d' \,\rrbracket \rightsquigarrow_{prg} \llbracket\, d'' \,\rrbracket$

Prove: $\forall po \in \llbracket\, d \,\rrbracket : 0 \notin \pi_2.po \Rightarrow \exists po'' \in \llbracket\, d'' \,\rrbracket : po \rightsquigarrow_{prr} po''$

⟨2⟩1. Assume: $po \in \llbracket\, d \,\rrbracket$

Prove: $0 \notin \pi_2.po \Rightarrow \exists po'' \in \llbracket\, d'' \,\rrbracket : po \rightsquigarrow_{prr} po''$

⟨3⟩1. Assume: $0 \notin \pi_2.po$

Prove: $\exists po'' \in \llbracket\, d'' \,\rrbracket : po \rightsquigarrow_{prr} po''$

⟨4⟩1. Let: $po' \in \llbracket\, d' \,\rrbracket$ s.t. $po \rightsquigarrow_{prr} po'$

Proof: By assumption ⟨1⟩1, assumption ⟨2⟩1 and assumption ⟨3⟩1

⟨4⟩2. $\exists po'' \in \llbracket\, d'' \,\rrbracket : po' \rightsquigarrow_{prr} po''$

⟨5⟩1. $0 \notin \pi_2.po'$

Proof: By assumption ⟨3⟩1 and ⟨4⟩1

⟨5⟩2. Q.E.D.

Proof: By assumption ⟨1⟩1, ⟨4⟩1 and ⟨5⟩1

⟨4⟩3. Let: $po'' \in \llbracket\, d'' \,\rrbracket$ s.t. $po' \rightsquigarrow\rightsquigarrow_{prr} po''$

Proof: By ⟨4⟩2

⟨4⟩4. $po \rightsquigarrow_{prr} po''$

⟨5⟩1. $o \rightsquigarrow_{rr} o''$

⟨6⟩1. $o \rightsquigarrow_{rr} o' \wedge o' \rightsquigarrow_{rr} o''$

Proof: By ⟨4⟩1 and ⟨4⟩3

⟨6⟩2. Q.E.D.

Proof: By ⟨6⟩1 and Theorem 5 in [RRS07]

⟨5⟩2. $Q'' \subseteq Q$

Proof: By ⟨4⟩1 and ⟨4⟩3

⟨5⟩3. Q.E.D.

Proof: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩5. Q.E.D.

Proof: By ⟨4⟩3 ($po'' \in \llbracket\, d'' \,\rrbracket$) and ⟨4⟩4

⟨3⟩2. Q.E.D.

Proof: ⇒-rule

⟨2⟩2. Q.E.D.

Proof: ∀-rule

⟨1⟩2. Q.E.D.

Proof: ⇒-rule

□

**Theorem 12 (Transitivity of $\rightsquigarrow_{pl}$).** *Let $d$, $d'$ and $d''$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\, d \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d' \,\rrbracket \wedge \llbracket\, d' \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d'' \,\rrbracket \Rightarrow \llbracket\, d \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d'' \,\rrbracket$$

Proof.

⟨1⟩1. Assume: $\llbracket\, d \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d' \,\rrbracket \wedge \llbracket\, d' \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d'' \,\rrbracket$

1. $\llbracket\, d \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d' \,\rrbracket$
2. $\llbracket\, d' \,\rrbracket \rightsquigarrow_{pl} \llbracket\, d'' \,\rrbracket$

Prove: $[\![ d ]\!] \rightsquigarrow_{pl} [\![ d'' ]\!]$

⟨2⟩1. $[\![ d ]\!] \rightsquigarrow_{pg} [\![ d'' ]\!]$

Proof: By assumptions ⟨1⟩1.1, ⟨1⟩1.2 and transitivity of $\rightsquigarrow_{pg}$ (Theorem 1 in [RHS05].)

⟨2⟩2. $\forall po'' \in [\![ d'' ]\!] : \exists S'' \subseteq [\![ d'' ]\!] : \exists po \in [\![ d ]\!] : po'' \in S'' \wedge po \rightsquigarrow_{pr} \bar{\oplus} S''$

⟨3⟩1. Assume: $po'' \in [\![ d'' ]\!]$

Prove: $\exists S'' \subseteq [\![ d'' ]\!] : \exists po \in [\![ d ]\!] : po'' \in S'' \wedge po \rightsquigarrow_{pr} \bar{\oplus} S''$

⟨4⟩1. $\exists po \in [\![ d ]\!] : po \rightsquigarrow_{pr} \bar{\oplus}[\![ d'' ]\!]$

⟨5⟩1. Let: $po \in [\![ d ]\!]$ such that $po \rightsquigarrow_{pr} \bar{\oplus}[\![ d ]\!]$

Proof: By Lemma 11

⟨5⟩2. $\pi_1.po \rightsquigarrow_r \pi_1.\bar{\oplus}[\![ d'' ]\!]$

⟨6⟩1. $\pi_1.\bar{\oplus}[\![ d ]\!] \rightsquigarrow_r \pi_1.\bar{\oplus}[\![ d' ]\!]$

Proof: By assumption ⟨1⟩1.1 and Lemma 1

⟨6⟩2. $\pi_1.\bar{\oplus}[\![ d' ]\!] \rightsquigarrow_r \pi_1.\bar{\oplus}[\![ d'' ]\!]$

Proof: By assumption ⟨1⟩1.2 and Lemma 1

⟨6⟩3. Q.E.D.

Proof: By ⟨5⟩1, ⟨6⟩1, ⟨6⟩2 and transitivity of $\rightsquigarrow_r$

⟨5⟩3. $\pi_2.\bar{\oplus}[\![ d'' ]\!] \subseteq \pi_2.po$

⟨6⟩1. $1 \in \pi_2.\bar{\oplus}[\![ d'' ]\!] \Rightarrow 1 \in \pi_2.po$

⟨7⟩1. Assume: $1 \in \pi_2.\bar{\oplus}[\![ d'' ]\!]$

Prove: $1 \in \pi_2.po$

⟨8⟩1. Let: $po''_1 \in [\![ d'' ]\!]$ such that $po''_1 \rightsquigarrow_{pr} \bar{\oplus}[\![ d'' ]\!]$

Proof: By Lemma 11

⟨8⟩2. $\forall po_1 \in [\![ d'' ]\!] : \pi_2.po_1 \neq \emptyset$

Proof: By assumption ⟨7⟩1 (since $\pi_2.\bar{\oplus}[\![ d'' ]\!] \neq \emptyset$)

⟨8⟩3. $1 \in \pi_2.po''_1$

Proof: By assumption ⟨7⟩1 and ⟨8⟩1

⟨8⟩4. $\forall S \subseteq [\![ d'' ]\!] : po''_1 \in S \Rightarrow 1 \in \pi_2.\bar{\oplus} S$

Proof: By ⟨8⟩2, ⟨8⟩3 and definition 7

⟨8⟩5. Let: $po'_1 \in [\![ d' ]\!], S''_1 \subseteq [\![ d'' ]\!]$ such that
$po''_1 \in S''_1 \wedge po'_1 \rightsquigarrow_{pr} \bar{\oplus} S''_1$

Proof: By assumption ⟨1⟩1.2

⟨8⟩6. $1 \in \pi_2.po'_1$

Proof: By ⟨8⟩4 and ⟨8⟩5

⟨8⟩7. $\forall po \in [\![ d' ]\!] : \pi_2.po \neq \emptyset$

Proof: By ⟨8⟩2 and assumption ⟨1⟩1.2 (since every p-obligation in $[\![ d' ]\!]$ either has 0 in its set of probabilities or must be represented in $[\![ d'' ]\!]$, and all combinations of p-obligations in $[\![ d'' ]\!]$ will have a non-empty probability set because of ⟨8⟩2).

⟨8⟩8. $\forall S \subseteq [\![ d' ]\!] : po'_1 \in S \Rightarrow 1 \in \pi_2.\bar{\oplus} S$

Proof: By ⟨8⟩6 and ⟨8⟩7

⟨8⟩9. Let: $po_1 \in [\![ d ]\!], S'_1 \subseteq [\![ d' ]\!]$ such that $po'_1 \in S'_1 \wedge po_1 \rightsquigarrow_{pr} \bar{\oplus} S'_1$

Proof: By assumption ⟨1⟩1.1

⟨8⟩10. $1 \in \pi_2.po_1$

Proof: By $\langle 8\rangle 8$ and $\langle 8\rangle 9$

$\langle 8\rangle 11.$ $\forall po \in \llbracket\, d \,\rrbracket : \pi_2.po \neq \emptyset$

Proof: By $\langle 8\rangle 7$ and assumption $\langle 1\rangle 1.1$ (with similar comment as $\langle 8\rangle 7$).

$\langle 8\rangle 12.$ $1 \in \pi_2.\bar{\oplus}\llbracket\, d \,\rrbracket$

Proof: By $\langle 8\rangle 10$ and $\langle 8\rangle 11$, since $po_1 \in \llbracket\, d \,\rrbracket$

$\langle 8\rangle 13.$ Q.E.D.

Proof: By $\langle 8\rangle 12$ and $\langle 5\rangle 1$

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

Proof: $\Rightarrow$-rule

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

Proof: By $\langle 6\rangle 1$ and Lemma 2

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

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 3$

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

Proof: By $\langle 4\rangle 1$; $\llbracket\, d'' \,\rrbracket$ is the $S''$ we are looking for.

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

Proof: $\forall$-rule

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

Proof: By $\langle 2\rangle 1$, $\langle 2\rangle 2$ and definition 25

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

Proof: $\Rightarrow$-rule

□

**Theorem 13 (Non-transitivity of $\rightsquigarrow_{prl}$).** *There exists sequence diagrams $d$, $d'$ and $d''$ in $\mathcal{D}^p$ such that $\llbracket\, d \,\rrbracket \rightsquigarrow_{prl} \llbracket\, d' \,\rrbracket \wedge \llbracket\, d' \,\rrbracket \rightsquigarrow_{prl} \llbracket\, d'' \,\rrbracket \wedge \llbracket\, d \,\rrbracket \not\rightsquigarrow_{prl} \llbracket\, d'' \,\rrbracket$*

Proof. To see this, let

$$\begin{aligned} d &= a \\ d' &= \mathsf{palt}(a;\langle 0,1]\,,(a \;\mathsf{alt}\; b);\langle 0,1]) \\ d'' &= \mathsf{palt}((a \;\mathsf{alt}\; (\mathsf{refuse}\; b));\{1\},(b \;\mathsf{alt}\; (\mathsf{refuse}\; a));\{0\}) \end{aligned}$$

This means that

$$\begin{aligned} \llbracket\, d \,\rrbracket &= \{po_1\} \\ \llbracket\, d' \,\rrbracket &= \{po_1, po_2, po_3\} \\ \llbracket\, d'' \,\rrbracket &= \{po_4, po_5, po_6\} \end{aligned}$$

where

$$\begin{aligned} po_1 &= ((\{\langle a\rangle\}, \emptyset), \{1\}) \\ po_2 &= ((\{\langle a\rangle\}, \emptyset), \langle 0,1]) \\ po_3 &= ((\{\langle a\rangle\,, \langle b\rangle\}, \emptyset), \langle 0,1]) \\ po_4 &= ((\{\langle a\rangle\}, \{\langle b\rangle\}), \{1\}) \\ po_5 &= ((\{\langle b\rangle\}, \{\langle a\rangle\}), \{0\}) \\ po_6 &= ((\{\langle a\rangle\,, \langle b\rangle\}, \emptyset), \{1\}) \end{aligned}$$

Then $po_1 \rightsquigarrow_{prr} po_1$ and $po_1 \rightsquigarrow_{prr} \bar{\oplus}\{po_1, po_2, po_3\}$, so $\llbracket\ d\ \rrbracket \rightsquigarrow_{prl} \llbracket\ d'\ \rrbracket$. Furthermore, we have $po_1 \rightsquigarrow_{prr} po_4$, $po_2 \rightsquigarrow_{prr} po_4$, $po_3 \rightsquigarrow_{prr} po_4$ and $po_3 \rightsquigarrow_{prr} \bar{\oplus}\{po_4, po_5, po_6\}$, which means that $\llbracket\ d'\ \rrbracket \rightsquigarrow_{prl} \llbracket\ d''\ \rrbracket$. But there is no $S \subseteq \llbracket\ d''\ \rrbracket$ such that $po_1 \rightsquigarrow_{prr} \bar{\oplus}S$ and $S$ contains $po_6$, since $\langle b \rangle$ will be positive in $\bar{\oplus}S$ for any such $S$. So the p-obligation $po_6$ is not a member of any subset of $\llbracket\ d''\ \rrbracket$ whose combination is a refinement of a p-obligation in $\llbracket\ d\ \rrbracket$ according to $\rightsquigarrow_{prr}$.

□

**Theorem 14 (Transitivity of $\rightsquigarrow_{png}$).** *Let $d$, $d'$ and $d''$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d\ \rrbracket \rightsquigarrow_{png} \llbracket\ d'\ \rrbracket \wedge \llbracket\ d'\ \rrbracket \rightsquigarrow_{png} \llbracket\ d''\ \rrbracket \Rightarrow \llbracket\ d\ \rrbracket \rightsquigarrow_{png} \llbracket\ d''\ \rrbracket$$

Proof. The proof is similar to the proof of Theorem 11, just replace $\rightsquigarrow_{prr}$ with $\rightsquigarrow_{pnr}$ and $\rightsquigarrow_{prg}$ with $\rightsquigarrow_{png}$. In addition, refer to Theorem 5 in this paper instead of Theorem 5 in [RRS07].

□

**Theorem 15 (Transitivity of $\rightsquigarrow_{pnl}$).** *Let $d$, $d'$ and $d''$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'\ \rrbracket \wedge \llbracket\ d'\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d''\ \rrbracket \Rightarrow \llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d''\ \rrbracket$$

Proof.

$\langle 1 \rangle 1.$ Assume: 1. $\llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'\ \rrbracket$
2. $\llbracket\ d'\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d''\ \rrbracket$
Prove: $\llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d''\ \rrbracket$

$\langle 2 \rangle 1.$ $\llbracket\ d\ \rrbracket \rightsquigarrow_{png} \llbracket\ d''\ \rrbracket$
Proof: By assumptions $\langle 1 \rangle 1.1$, $\langle 1 \rangle 1.2$ and Theorem 14

$\langle 2 \rangle 2.$ $\forall po'' \in \llbracket\ d''\ \rrbracket : \exists S'' \subseteq \llbracket\ d''\ \rrbracket : \exists po \in \llbracket\ d\ \rrbracket : po'' \in S'' \wedge po \rightsquigarrow_{pnr} \bar{\oplus}S''$

$\langle 3 \rangle 1.$ Assume: $po'' \in \llbracket\ d''\ \rrbracket$
Prove: $\exists S'' \subseteq \llbracket\ d''\ \rrbracket : \exists po \in \llbracket\ d\ \rrbracket : po'' \in S'' \wedge po \rightsquigarrow_{pnr} \bar{\oplus}S''$

$\langle 4 \rangle 1.$ $\exists po \in \llbracket\ d\ \rrbracket : po \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d''\ \rrbracket$

$\langle 5 \rangle 1.$ Let: $po \in \llbracket\ d\ \rrbracket$ such that $po \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d\ \rrbracket$
Proof: By Lemma 12

$\langle 5 \rangle 2.$ $\pi_1.po \rightsquigarrow_{nr} \pi_1.\bar{\oplus}\llbracket\ d''\ \rrbracket$

$\langle 6 \rangle 1.$ $\pi_1.\bar{\oplus}\llbracket\ d\ \rrbracket \rightsquigarrow_{nr} \pi_1.\bar{\oplus}\llbracket\ d'\ \rrbracket$
Proof: By assumption $\langle 1 \rangle 1.1$ and Lemma 13

$\langle 6 \rangle 2.$ $\pi_1.\bar{\oplus}\llbracket\ d'\ \rrbracket \rightsquigarrow_{nr} \pi_1.\bar{\oplus}\llbracket\ d''\ \rrbracket$
Proof: By assumption $\langle 1 \rangle 1.2$ and Lemma 13

$\langle 6 \rangle 3.$ Q.E.D.
Proof: By $\langle 5 \rangle 1$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$ and Theorem 5

$\langle 5 \rangle 3.$ $\pi_2.\bar{\oplus}\llbracket\ d''\ \rrbracket \subseteq \pi_2.po$

$\langle 6 \rangle 1.$ $1 \in \pi_2.\bar{\oplus}\llbracket\ d''\ \rrbracket \Rightarrow 1 \in \pi_2.po$

$\langle 7 \rangle 1.$ Assume: $1 \in \pi_2.\bar{\oplus}\llbracket\ d''\ \rrbracket$
Prove: $1 \in \pi_2.po$

$\langle 8 \rangle 1.$ Let: $po''_1 \in \llbracket\ d''\ \rrbracket$ such that $po''_1 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d''\ \rrbracket$

PROOF: By Lemma 12

$\langle 8\rangle 2.$ $\forall po_1 \in \llbracket\ d''\ \rrbracket : \pi_2.po_1 \neq \emptyset$

PROOF: By assumption $\langle 7\rangle 1$ (since $\pi_2.\bar{\oplus}\llbracket\ d''\ \rrbracket \neq \emptyset$)

$\langle 8\rangle 3.$ $1 \in \pi_2.po_1''$

PROOF: By assumption $\langle 7\rangle 1$ and $\langle 8\rangle 1$

$\langle 8\rangle 4.$ $\forall S \subseteq \llbracket\ d''\ \rrbracket : po_1'' \in S \Rightarrow 1 \in \pi_2.\bar{\oplus} S$

PROOF: By $\langle 8\rangle 2$, $\langle 8\rangle 3$ and definition 7

$\langle 8\rangle 5.$ LET: $po_1' \in \llbracket\ d'\ \rrbracket, S_1'' \subseteq \llbracket\ d''\ \rrbracket$ such that $po_1'' \in S_1'' \wedge$
$po_1' \leadsto_{pnr} \bar{\oplus} S_1''$

PROOF: By assumption $\langle 1\rangle 1.2$

$\langle 8\rangle 6.$ $1 \in \pi_2.po_1'$

PROOF: By $\langle 8\rangle 4$ and $\langle 8\rangle 5$

$\langle 8\rangle 7.$ $\forall po \in \llbracket\ d'\ \rrbracket : \pi_2.po \neq \emptyset$

PROOF: By $\langle 8\rangle 2$ and assumption $\langle 1\rangle 1.2$ (since every p-obligation in $\llbracket\ d'\ \rrbracket$ either has 0 in its probability set or must be represented in $\llbracket\ d''\ \rrbracket$, and all combinations of p-obligations in $\llbracket\ d''\ \rrbracket$ will have a non-empty probability set because of $\langle 8\rangle 2$).

$\langle 8\rangle 8.$ $\forall S \subseteq \llbracket\ d'\ \rrbracket : po_1' \in S \Rightarrow 1 \in \pi_2.\bar{\oplus} S$

PROOF: By $\langle 8\rangle 6$ and $\langle 8\rangle 7$

$\langle 8\rangle 9.$ LET: $po_1 \in \llbracket\ d\ \rrbracket, S_1' \subseteq \llbracket\ d'\ \rrbracket$ such that
$po_1' \in S_1' \wedge po_1 \leadsto_{pnr} \bar{\oplus} S_1'$

PROOF: By assumption $\langle 1\rangle 1.1$

$\langle 8\rangle 10.$ $1 \in \pi_2.po_1$

PROOF: By $\langle 8\rangle 8$ and $\langle 8\rangle 9$

$\langle 8\rangle 11.$ $\forall po \in \llbracket\ d\ \rrbracket : \pi_2.po \neq \emptyset$

PROOF: By $\langle 8\rangle 7$ and assumption $\langle 1\rangle 1.1$ (with similar comment as $\langle 8\rangle 7$).

$\langle 8\rangle 12.$ $1 \in \pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket$

PROOF: By $\langle 8\rangle 10$ and $\langle 8\rangle 11$, since $po_1 \in \llbracket\ d\ \rrbracket$

$\langle 8\rangle 13.$ Q.E.D.

PROOF: By $\langle 8\rangle 12$ and $\langle 5\rangle 1$

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

PROOF: $\Rightarrow$-rule

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

PROOF: By $\langle 6\rangle 1$ and Lemma 2

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

PROOF: By $\langle 5\rangle 2$ and $\langle 5\rangle 3$

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

PROOF: By $\langle 4\rangle 1$; $\llbracket\ d''\ \rrbracket$ is the $S''$ we are looking for.

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

PROOF: $\forall$-rule

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

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$ and definition 25

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

PROOF: $\Rightarrow$-rule

□

### Transitivity between refinement and compliance

**Theorem 16 (Transitivity between refinement and compliance for $\rightsquigarrow_{pg}$).** *Let $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![ d_1 ]\!] \rightsquigarrow_{pg} [\![ d_2 ]\!] \wedge [\![ d_2 ]\!] \mapsto_{pg} \langle I \rangle_{d_2} \Rightarrow [\![ d_1 ]\!] \mapsto_{pg} \langle I \rangle_{d_1}$$

Proof.

$\langle 1 \rangle 1.$ Assume: $[\![ d_1 ]\!] \rightsquigarrow_{pg} [\![ d_2 ]\!] \wedge [\![ d_2 ]\!] \mapsto_{pg} \langle I \rangle_{d_2}$
Prove: $[\![ d_1 ]\!] \mapsto_{pg} \langle I \rangle_{d_1}$

$\langle 2 \rangle 1.$ $\forall po \in [\![ d_1 ]\!] : 0 \notin \pi_2.po \Rightarrow \exists po' \in \langle I \rangle_{d_1} : po \mapsto_{pr} po'$

$\langle 3 \rangle 1.$ Assume: $po_1 \in [\![ d_1 ]\!]$
Prove: $0 \notin \pi_2.po_1 \Rightarrow \exists po' \in \langle I \rangle_{d_1} : po_1 \mapsto_{pr} po'$

$\langle 4 \rangle 1.$ Assume: $0 \notin \pi_2.po_1$
Prove: $\exists po' \in \langle I \rangle_{d_1} : po_1 \mapsto_{pr} po'$

$\langle 5 \rangle 1.$ Let: $po_2 \in [\![ d_2 ]\!]$ such that $po_1 \rightsquigarrow_{pr} po_2$
Proof: By assumptions $\langle 1 \rangle 1$, $\langle 3 \rangle 1$ and $\langle 4 \rangle 1$

$\langle 5 \rangle 2.$ $0 \notin \pi_2.po_2$
Proof: By $\langle 5 \rangle 1$ and assumption $\langle 4 \rangle 1$

$\langle 5 \rangle 3.$ Let: $po_2' \in \langle I \rangle_{d_2}$ such that $po_2 \mapsto_{pr} po_2'$
Proof: By $\langle 5 \rangle 1$, $\langle 5 \rangle 2$ and assumption $\langle 1 \rangle 1$

$\langle 5 \rangle 4.$ $po_1 \mapsto_{pr} po_2'$
Proof: By $\langle 5 \rangle 1$, $\langle 5 \rangle 3$ and Lemma 1 in [RHS07a] (transitivity of $\rightsquigarrow_{pr}$), as $\mapsto_{pr}$ is identical with $\rightsquigarrow_{pr}$

$\langle 5 \rangle 5.$ Let: $po_1' = ((p_2', n_2' \cap \mathcal{H}^{ll(d_1)}), Q_2')$

$\langle 5 \rangle 6.$ $po_1' \in \langle I \rangle_{d_1}$
Proof: By $\langle 5 \rangle 5$, $\langle 5 \rangle 3$ and definition 30 (notice that $traces(I)$ and $\mathcal{F}_I$ are independent of $d_1$ and $d_2$, therefore $\langle I \rangle_{d_1}$ and $\langle I \rangle_{d_2}$ only differ w.r.t. the negative sets)

$\langle 5 \rangle 7.$ $po_1 \mapsto_{pr} po_1'$

$\langle 6 \rangle 1.$ $(p_1, n_1) \mapsto_r (p_2', n_2')$
Proof: By $\langle 5 \rangle 4$

$\langle 6 \rangle 2.$ $p_1 \cup n_1 \subseteq \mathcal{H}^{ll(d_1)}$
Proof: By assumption $\langle 3 \rangle 1$

$\langle 6 \rangle 3.$ $(p_1, n_1) \mapsto_r (p_2', n_2' \cap \mathcal{H}^{ll(d_1)})$
Proof: By $\langle 6 \rangle 1$ and $\langle 6 \rangle 2$

$\langle 6 \rangle 4.$ $Q_2' \subseteq Q_1$
Proof: By $\langle 5 \rangle 4$

$\langle 6 \rangle 5.$ Q.E.D.
Proof: By $\langle 6 \rangle 3$ and $\langle 6 \rangle 4$

$\langle 5 \rangle 8.$ Q.E.D.
Proof: By $\langle 5 \rangle 6$ and $\langle 5 \rangle 7$; $po_1'$ is the $po'$ we are looking for

$\langle 4 \rangle 2.$ Q.E.D.
Proof: $\Rightarrow$-rule

⟨3⟩2. Q.E.D.

PROOF: ∀-rule

⟨2⟩2. Q.E.D.

PROOF: By ⟨2⟩1

⟨1⟩2. Q.E.D.

PROOF: ⇒-rule

□

**Theorem 17 (Transitivity between refinement and compliance for $\rightsquigarrow_{prg}$).** *Let $d_1$ and $d_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{prg} \langle I \rangle_{d_2} \Rightarrow \llbracket\ d_1\ \rrbracket \mapsto_{prg} \langle I \rangle_{d_1}$$

PROOF.

The proof is similar to the proof for Theorem 16; just replace $\rightsquigarrow_{pr}$ with $\rightsquigarrow_{prr}$ and $\mapsto_{pr}$ with $\mapsto_{prr}$. In addition, refer to Lemma 15 in step ⟨5⟩4.

□

**Theorem 18 (Transitivity between refinement and compliance for $\rightsquigarrow_{pl}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{pl} \langle I \rangle_{d_2} \Rightarrow \llbracket\ d_1\ \rrbracket \mapsto_{pl} \langle I \rangle_{d_1}$$

PROOF.

⟨1⟩1. ASSUME: $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{pl} \langle I \rangle_{d_2}$

PROVE: $\llbracket\ d_1\ \rrbracket \mapsto_{pl} \langle I \rangle_{d_1}$

⟨2⟩1. $\llbracket\ d_1\ \rrbracket \mapsto_{pg} \langle I \rangle_{d_1}$

PROOF: By assumption ⟨1⟩1 and Theorem 16

⟨2⟩2. $\forall po_1' \in \langle I \rangle_{d_1} : \exists S \subseteq \langle I \rangle_{d_1}, po_1 \in \llbracket\ d_1\ \rrbracket : po_1 \mapsto_{pr} \bar{\oplus} S$

⟨3⟩1. ASSUME: $po_1' \in \langle I \rangle_{d_1}$

PROVE: $\exists S \subseteq \langle I \rangle_{d_1}, po_1 \in \llbracket\ d_1\ \rrbracket : po_1 \mapsto_{pr} \bar{\oplus} S$

⟨4⟩1. $\forall po \in \langle I \rangle_{d_2} : \pi_2.po \neq \emptyset$

PROOF: By definition 30

⟨4⟩2. $\forall po \in \llbracket\ d_2\ \rrbracket : \pi_2.po \neq \emptyset$

PROOF: By ⟨4⟩1 and assumption ⟨1⟩1 (since every p-obligation in $\llbracket\ d_2\ \rrbracket$ either has 0 in its set of probabilities or is represented in $\langle I \rangle_{d_2}$)

⟨4⟩3. $\forall po \in \llbracket\ d_1\ \rrbracket : \pi_2.po \neq \emptyset$

PROOF: By ⟨4⟩2 and assumption ⟨1⟩1 (since every p-obligation in $\llbracket\ d_1\ \rrbracket$ either has 0 in its set of probabilities or is represented in $\llbracket\ d_2\ \rrbracket$)

⟨4⟩4. $\pi_2.\bar{\oplus}\llbracket\ d_1\ \rrbracket = \{1\}$

PROOF: By ⟨4⟩3 and Lemma 2

⟨4⟩5. $\pi_2.\bar{\oplus}\langle I \rangle_{d_1} = \{1\}$

PROOF: By definition 30 and definition 7, since $f_I$ is a measure

⟨4⟩6. $\pi_2.\bar{\oplus}\langle I \rangle_{d_1} \subseteq \pi_2.\bar{\oplus}\llbracket\ d_1\ \rrbracket$

PROOF: By ⟨4⟩4 and ⟨4⟩5

⟨4⟩7. $\oplus\llbracket\ d_1\ \rrbracket \mapsto_r \oplus\langle I \rangle_{d_1}$

Proof: By assumption ⟨1⟩1 and Lemma 17

⟨4⟩8. $\bar{\oplus}\llbracket\ d_1\ \rrbracket \mapsto_{pr} \bar{\oplus}\langle I\rangle_{d_1}$

Proof: By ⟨4⟩6 and ⟨4⟩7

⟨4⟩9. Let: $po \in \llbracket\ d_1\ \rrbracket$ such that $po \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket$

Proof: By Lemma 11

⟨4⟩10. $po \mapsto_{pr} \bar{\oplus}\langle I\rangle_{d_1}$

Proof: By ⟨4⟩8, ⟨4⟩9 and Lemma 1 in [RHS07a] (transitivity of $\rightsquigarrow_{pr}$), as $\mapsto_{pr}$ is identical with $\rightsquigarrow_{pr}$

⟨4⟩11. Q.E.D.

Proof: By ⟨4⟩9 and ⟨4⟩10; $po$ is the $po_1$ we are looking for and $\langle I\rangle_{d_1}$ is the $S$ we are looking for

⟨3⟩2. Q.E.D.

Proof: ∀-rule

⟨2⟩3. Q.E.D.

Proof: By ⟨2⟩1 and ⟨2⟩2

⟨1⟩2. Q.E.D.

Proof: ⇒-rule

□

**Theorem 19 (Transitivity between refinement and compliance for $\rightsquigarrow_{png}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{png} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{png} \langle I\rangle_{d_2} \Rightarrow \llbracket\ d_1\ \rrbracket \mapsto_{png} \langle I\rangle_{d_1}$$

Proof.

⟨1⟩1. Assume: $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{png} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{png} \langle I\rangle_{d_2}$

Prove: $\llbracket\ d_1\ \rrbracket \mapsto_{png} \langle I\rangle_{d_1}$

⟨2⟩1. $\llbracket\ d_1\ \rrbracket \mapsto_{prg} \langle I\rangle_{d_1}$

⟨3⟩1. $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{prg} \langle I\rangle_{d_2}$

Proof: By assumption ⟨1⟩1, definition 24 and definition 35

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1 and Theorem 17

⟨2⟩2. Q.E.D.

Proof: By ⟨2⟩1 and definition 35

⟨1⟩2. Q.E.D.

Proof: ⇒-rule

□

**Theorem 20 (Transitivity between refinement and compliance for $\rightsquigarrow_{pnl}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{pnl} \langle I\rangle_{d_2} \Rightarrow \llbracket\ d_1\ \rrbracket \mapsto_{pnl} \langle I\rangle_{d_1}$$

Proof.

⟨1⟩1. Assume: $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{pnl} \langle I\rangle_{d_2}$

Prove: $\llbracket\ d_1\ \rrbracket \mapsto_{pnl} \langle I\rangle_{d_1}$

$\langle 2\rangle 1.$ $\llbracket\ d_1\ \rrbracket \mapsto_{png} \langle I\rangle_{d_1}$

$\langle 3\rangle 1.$ $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{png} \llbracket\ d_2\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \mapsto_{png} \langle I\rangle_{d_2}$

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

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

PROOF: By $\langle 3\rangle 1$ and Theorem 19

$\langle 2\rangle 2.$ $\forall po' \in \langle I\rangle_{d_1} : \exists S \subseteq \langle I\rangle_{d_1} : \exists po \in \llbracket\ d_1\ \rrbracket : po' \in S \wedge po \mapsto_{prr} \bar{\oplus} S$

$\langle 3\rangle 1.$ ASSUME: $po'_1 \in \langle I\rangle_{d_1}$

PROVE: $\exists S \subseteq \langle I\rangle_{d_1} : \exists po \in \llbracket\ d_1\ \rrbracket : po'_1 \in S \wedge po \mapsto_{prr} \bar{\oplus} S$

$\langle 4\rangle 1.$ LET: $po_1 \in \llbracket\ d_1\ \rrbracket$ such that $po_1 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_1\ \rrbracket$

PROOF: By Lemma 12

$\langle 4\rangle 2.$ $po_1 \mapsto_{prr} \bar{\oplus}\langle I\rangle_{d_1}$

$\langle 5\rangle 1.$ LET: $((p_3, n_3), Q_3) = \bar{\oplus}\llbracket\ d_1\ \rrbracket$<br>
$((p_4, n_4), Q_4) = \bar{\oplus}\llbracket\ d_2\ \rrbracket$<br>
$((p_5, n_5), Q_5) = \bar{\oplus}\langle I\rangle_{d_1}$<br>
$((p_6, n_6), Q_6) = \bar{\oplus}\langle I\rangle_{d_2}$

$\langle 5\rangle 2.$ $(p_3, n_3) \mapsto_{rr} (p_5, n_5)$

$\langle 6\rangle 1.$ $(p_3, n_3) \rightsquigarrow_{nr} (p_4, n_4)$

PROOF: By assumption $\langle 1\rangle 1$ and Lemma 13

$\langle 6\rangle 2.$ $(p_3, n_3) \mapsto_{r} (p_5, n_5)$

$\langle 7\rangle 1.$ $n_3 \subseteq n_5$

$\langle 8\rangle 1.$ ASSUME: $t \in n_3$

PROVE: $t \in n_5$

$\langle 9\rangle 1.$ $t \in n_4$

PROOF: By assumption $\langle 8\rangle 1$ and $\langle 6\rangle 1$

$\langle 9\rangle 2.$ $\forall po \in \llbracket\ d_2\ \rrbracket : t \in n$

PROOF: By $\langle 9\rangle 1$

$\langle 9\rangle 3.$ $\forall po \in \langle I\rangle_{d_2} : t \in n$

$\langle 10\rangle 1.$ ASSUME: $\exists po \in \langle I\rangle_{d_2} : t \notin n$

PROVE: $\perp$

$\langle 11\rangle 1.$ LET: $po''_2 \in \langle I\rangle_{d_2}$ such that $t \notin n$

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

$\langle 11\rangle 2.$ LET: $S_2 \subseteq \langle I\rangle_{d_2}, po'_2 \in \llbracket\ d_2\ \rrbracket$ such that $po''_2 \in S_2 \wedge po'_2 \mapsto_{prr} \bar{\oplus} S_2$

PROOF: By assumption $\langle 1\rangle 1$ ($\llbracket\ d_2\ \rrbracket \mapsto_{prr} \langle I\rangle_{d_2}$)

$\langle 11\rangle 3.$ $t \notin \pi_2. \oplus S_2$

PROOF: By $\langle 11\rangle 1$ and $\langle 11\rangle 2$

$\langle 11\rangle 4.$ $t \notin n'_2$

PROOF: By $\langle 11\rangle 2$ and $\langle 11\rangle 3$

$\langle 11\rangle 5.$ Q.E.D.

PROOF: By $\langle 11\rangle 4$ and $\langle 9\rangle 2$

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

PROOF: $\perp$-rule

$\langle 9\rangle 4.$ $t \in n_6$

PROOF: By $\langle 9\rangle 3$

$\langle 9\rangle 5.$ $t \in \mathcal{H}^{ll(d_1)}$

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

$\langle 9\rangle 6$. $(n_6 \setminus n_5) \cap \mathcal{H}^{ll(d_1)} = \emptyset$

PROOF: By definition 4 and definition 30

$\langle 9\rangle 7$. Q.E.D.

PROOF: By $\langle 9\rangle 4$, $\langle 9\rangle 5$ and $\langle 9\rangle 6$

$\langle 8\rangle 2$. Q.E.D.

PROOF: $\subseteq$-rule

$\langle 7\rangle 2$. $p_3 \subseteq p_5 \cup n_5$

$\langle 8\rangle 1$. ASSUME: $t \in p_3$
PROVE: $t \in p_5 \cup n_5$

$\langle 9\rangle 1$. $t \in p_4 \cup n_4$

PROOF: By assumption $\langle 8\rangle 1$ and $\langle 6\rangle 1$

$\langle 9\rangle 2$. $\forall po \in [\![ d_2 ]\!] : t \in p \cup n$

PROOF: By $\langle 9\rangle 1$

$\langle 9\rangle 3$. $\forall po \in \langle I\rangle_{d_2} : t \in p \cup n$

$\langle 10\rangle 1$. ASSUME: $\exists po \in \langle I\rangle_{d_2}$ such that $t \notin p \cup n$
PROVE: $\perp$

$\langle 11\rangle 1$. LET: $po''_2 \in \langle I\rangle_{d_2}$ such that $t \notin p''_2 \cup n''_2$

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

$\langle 11\rangle 2$. LET: $S_2 \subseteq \langle I\rangle_{d_2}, po'_2 \in [\![ d_2 ]\!]$ such that $po''_2 \in S_2 \wedge po'_2 \mapsto_{prr} \bar{\oplus} S_2$

PROOF: By assumption $\langle 1\rangle 1$ ($[\![ d_2 ]\!] \mapsto_{pnl} \langle I\rangle_{d_2}$)

$\langle 11\rangle 3$. $t \notin \pi_1.\oplus S_2 \cup \pi_2.\oplus S_2$

PROOF: By $\langle 11\rangle 1$ and $\langle 11\rangle 2$

$\langle 11\rangle 4$. $t \notin p'_2 \cup n'_2$

PROOF: By $\langle 11\rangle 2$ and $\langle 11\rangle 3$

$\langle 11\rangle 5$. Q.E.D.

PROOF: By $\langle 11\rangle 4$ and $\langle 9\rangle 2$

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

PROOF: $\perp$-rule

$\langle 9\rangle 4$. $t \in p_6 \cup n_6$

PROOF: By $\langle 9\rangle 3$

$\langle 9\rangle 5$. $t \in \mathcal{H}^{ll(d_1)}$

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

$\langle 9\rangle 6$. $((p_6 \cup n_6) \setminus (p_5 \cup n_5)) \cap \mathcal{H}^{ll(d_1)} = \emptyset$

PROOF: By definition 4 and definition 30

$\langle 9\rangle 7$. Q.E.D.

PROOF: By $\langle 9\rangle 4$, $\langle 9\rangle 5$ and $\langle 9\rangle 6$

$\langle 8\rangle 2$. Q.E.D.

PROOF: $\subseteq$-rule

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

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

$\langle 6\rangle 3$. $p_3 \cap p_5 \neq \emptyset$

$\langle 7\rangle 1$. CASE: $traces(I)$ contains exactly one trace

$\langle 8\rangle 1$. LET: $\{t\} = traces(I)$

PROOF: By assumption ⟨7⟩1

⟨8⟩2. $\langle I \rangle_{d_1} = \{((\{t\}, \mathcal{H}^{ll(d_1)} \setminus \{t\}), \{1\})\}$

PROOF: By ⟨8⟩1 and definition 30

⟨8⟩3. $\langle I \rangle_{d_2} = \{((\{t\}, \mathcal{H}^{ll(d_2)} \setminus \{t\}), \{1\})\}$

PROOF: By ⟨8⟩1 and definition 30

⟨8⟩4. $t \in p_5$

PROOF: By ⟨8⟩2 and definition 4

⟨8⟩5. $t \in p_3$

⟨9⟩1. ASSUME: $t \notin p_3$

PROVE: $\perp$

⟨10⟩1. $(\exists po \in \llbracket\ d_1\ \rrbracket : t \notin p \cup n) \vee (\forall po \in \llbracket\ d_1\ \rrbracket : t \in n)$

PROOF: By assumption ⟨9⟩1

⟨10⟩2. CASE: $\exists po \in \llbracket\ d_1\ \rrbracket : t \notin p \cup n$

⟨11⟩1. LET: $po'_1 \in \llbracket\ d_1\ \rrbracket$ such that $po'_1 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_1\ \rrbracket$

PROOF: By Lemma 12

⟨11⟩2. $0 \notin Q'_1$

⟨12⟩1. $0 \notin \pi_2.\bar{\oplus}\llbracket\ d_1\ \rrbracket$

PROOF: By Lemma 2

⟨12⟩2. Q.E.D.

PROOF: By ⟨12⟩1 and ⟨11⟩1

⟨11⟩3. LET: $po'_2 \in \llbracket\ d_2\ \rrbracket$ such that $po'_1 \rightsquigarrow_{pnr} po'_2$

PROOF: By ⟨11⟩2 and assumption ⟨1⟩1

⟨11⟩4. $t \notin p'_2 \cup n'_2$

⟨12⟩1. $t \notin p_3 \cup n_3$

PROOF: By assumption ⟨10⟩2

⟨12⟩2. $t \notin p'_1 \cup n'_1$

PROOF: By ⟨12⟩1 and ⟨11⟩1

⟨12⟩3. Q.E.D.

PROOF: By ⟨12⟩2 and ⟨11⟩3

⟨11⟩5. $0 \notin Q'_2$

PROOF: By ⟨11⟩2 and ⟨11⟩3

⟨11⟩6. $\forall po \in \langle I \rangle_{d_2} : po'_2 \not\mapsto_{prr} po$

PROOF: By ⟨11⟩4 and ⟨8⟩3

⟨11⟩7. Q.E.D.

PROOF: By ⟨11⟩5, ⟨11⟩6 and assumption ⟨1⟩1 ($\llbracket\ d_2\ \rrbracket \mapsto_{pnl} \langle I \rangle_{d_2}$)

⟨10⟩3. CASE: $\forall po \in \llbracket\ d_1\ \rrbracket : t \in n$

⟨11⟩1. $\forall po \in \llbracket\ d_2\ \rrbracket : t \in n$

PROOF: By assumption ⟨10⟩3 and assumption ⟨1⟩1 ($\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnr} \llbracket\ d_2\ \rrbracket$)

⟨11⟩2. $\llbracket\ d_2\ \rrbracket \not\mapsto_{prr} \langle I \rangle_{d_2}$

PROOF: By ⟨11⟩1 and ⟨8⟩3

⟨11⟩3. Q.E.D.

PROOF: By ⟨11⟩2 and assumption ⟨1⟩1

⟨10⟩4. Q.E.D.

PROOF: By $\langle 10\rangle 1$ the cases $\langle 10\rangle 2$ and $\langle 10\rangle 3$ are exhaustive

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

PROOF: $\perp$-rule

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

PROOF: By $\langle 8\rangle 4$ and $\langle 8\rangle 5$

$\langle 7\rangle 2$. CASE: $traces(I)$ contains more than one trace

$\langle 8\rangle 1$. $p_5 \subseteq \mathcal{H}^{ll(d_1)}$

$\langle 9\rangle 1$. ASSUME: $t_1 \in p_5$
PROVE: $t_1 \in \mathcal{H}^{ll(d_1)}$

$\langle 10\rangle 1$. ASSUME: $t_1 \notin \mathcal{H}^{ll(d_1)}$
PROVE: $\perp$

$\langle 11\rangle 1$. $\forall po \in \langle I\rangle_{d_1} : t_1 \in p$

PROOF: By assumption $\langle 9\rangle 1$, assumption $\langle 10\rangle 1$ and definition 30 (since $t_1 \notin \mathcal{H}^{ll(d_1)}$, we have $\forall po \in \langle I\rangle_{d_1} : t_1 \notin n$)

$\langle 11\rangle 2$. LET: $t_2 \in traces(I)$ such that $t_1 \neq t_2$

PROOF: By assumption $\langle 7\rangle 2$

$\langle 11\rangle 3$. LET: $t_1', t_2'$ be finite traces such that $t_1' \sqsubseteq t_1 \wedge t_2' \sqsubseteq t_2 \wedge t_1' \neq t_2'$

PROOF: By $\langle 11\rangle 2$

$\langle 11\rangle 4$. $t_1 \notin c_{t_2'}$

PROOF: By $\langle 11\rangle 3$

$\langle 11\rangle 5$. $((c_{t_2'}, \mathcal{H}^{ll(d_1)} \setminus c_{t_2'}), f_I(c_{t_2'})) \in \langle I\rangle_{d_1}$

PROOF: By definition 30

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

PROOF: By $\langle 11\rangle 1$, $\langle 11\rangle 4$ and $\langle 11\rangle 5$

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

PROOF: $\perp$-rule

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

PROOF: $\subseteq$-rule

$\langle 8\rangle 2$. $p_4 \cap p_6 \neq \emptyset$

$\langle 9\rangle 1$. ASSUME: $p_4 \cap p_6 = \emptyset$
PROVE: $\perp$

$\langle 10\rangle 1$. $p_6 \subseteq \mathcal{H}^{ll(d_2)}$

PROOF: Similar to the proof for $\langle 8\rangle 1$

$\langle 10\rangle 2$. $traces(I) = p_6$

PROOF: By $\langle 10\rangle 1$ and definition 30

$\langle 10\rangle 3$. CASE: $n_4 \cap traces(I) = \emptyset$

$\langle 11\rangle 1$. LET: $po_2' \in [\![\ d_2\ ]\!]$ such that $po_2' \rightsquigarrow_{pnr} \bar{\oplus}[\![\ d_2\ ]\!]$

PROOF: By Lemma 12

$\langle 11\rangle 2$. $0 \notin Q_2'$

PROOF: By $\langle 11\rangle 1$ and Lemma 2

$\langle 11\rangle 3$. $p_4 \cap traces(I) = \emptyset$

PROOF: By $\langle 10\rangle 2$ and assumption $\langle 9\rangle 1$

$\langle 11\rangle 4$. $p_4 \cup n_4 = p_2' \cup n_2'$

Proof: By ⟨11⟩1

⟨11⟩5. $(p_4 \cup n_4) \cap traces(I) = \emptyset$

Proof: By ⟨11⟩3 and assumption ⟨10⟩3

⟨11⟩6. $p_2' \cap traces(I) = \emptyset$

Proof: By ⟨11⟩5 and ⟨11⟩4

⟨11⟩7. $\forall po \in \langle I \rangle_{d_2} : po_2' \not\mapsto_{prr} po$

Proof: By ⟨11⟩6

⟨11⟩8. Q.E.D.

Proof: By ⟨11⟩7, ⟨11⟩2 and assumption ⟨1⟩1 (second conjunct)

⟨10⟩4. Case: $n_4 \cap traces(I) \neq \emptyset$

⟨11⟩1. Let: $t \in n_4 \cap traces(I)$

Proof: By assumption ⟨10⟩4

⟨11⟩2. Let: $po_2'' \in \langle I \rangle_{d_2}$ such that $t \in p_2''$

Proof: By ⟨11⟩1 ($t \in traces(I)$)

⟨11⟩3. $t \notin n_2''$

Proof: By ⟨11⟩2 and definition 30 (every p-obligation in any $\langle I \rangle$ is consistent)

⟨11⟩4. Let: $S_2'' \subseteq \langle I \rangle_{d_2}, po_2''' \in [\![ \ d_2 \ ]\!]$ such that $p_2'' \in S_2'' \wedge po_2''' \mapsto_{prr} \bar{\oplus} S_2''$

Proof: By assumption ⟨1⟩1 (second conjunct)

⟨11⟩5. $t \notin \pi_2. \oplus S_2''$

Proof: By ⟨11⟩3 and ⟨11⟩4

⟨11⟩6. $t \in n_2'''$

Proof: By ⟨11⟩1

⟨11⟩7. Q.E.D.

Proof: By ⟨11⟩4, ⟨11⟩5 and ⟨11⟩6

⟨10⟩5. Q.E.D.

Proof: The cases ⟨10⟩3 and ⟨10⟩4 are exhaustive

⟨9⟩2. Q.E.D.

Proof: $\bot$-rule

⟨8⟩3. $p_4 \subseteq p_3$

Proof: By ⟨6⟩1

⟨8⟩4. $p_3 \cap p_6 \neq \emptyset$

Proof: By ⟨8⟩2 and ⟨8⟩3

⟨8⟩5. $p_3 \in \mathcal{H}^{ll(d_1)}$

Proof: By ⟨5⟩1

⟨8⟩6. $p_3 \cap p_6 \in \mathcal{H}^{ll(d_1)}$

Proof: By ⟨8⟩5

⟨8⟩7. $p_5 = p_6 \cap \mathcal{H}^{ll(d_1)}$

Proof: By ⟨8⟩1, definition 30 and definition 4

⟨8⟩8. Q.E.D.

Proof: By ⟨8⟩4, ⟨8⟩6 and ⟨8⟩7

⟨7⟩3. Q.E.D.

Proof: The cases ⟨7⟩1 and ⟨7⟩2 are exhaustive

$\langle 6\rangle 4.$ Q.E.D.

PROOF: By $\langle 6\rangle 2$ and $\langle 6\rangle 3$

$\langle 5\rangle 3.$ $Q_5 \subseteq Q_3$

$\langle 6\rangle 1.$ $\forall po \in \langle I\rangle_{d_2} : Q \neq \emptyset$

PROOF: By definition 30

$\langle 6\rangle 2.$ $\forall po \in [\![ \, d_2 \, ]\!] : Q \neq \emptyset$

PROOF: By $\langle 6\rangle 1$ and assumption $\langle 1\rangle 1$ ($[\![ \, d_2 \, ]\!] \mapsto_{pnl} \langle I\rangle_{d_2}$)

$\langle 6\rangle 3.$ $\forall po \in [\![ \, d_1 \, ]\!] : Q \neq \emptyset$

PROOF: By $\langle 6\rangle 2$ and assumption $\langle 1\rangle 1$ ($[\![ \, d_1 \, ]\!] \rightsquigarrow_{pnl} [\![ \, d_2 \, ]\!]$)

$\langle 6\rangle 4.$ $Q_3 \neq \emptyset$

PROOF: By $\langle 6\rangle 3$

$\langle 6\rangle 5.$ $Q_3 = \{1\}$

PROOF: By $\langle 6\rangle 4$ and Lemma 2

$\langle 6\rangle 6.$ $Q_5 = \{1\}$

PROOF: By definition 30 and definition 7

$\langle 6\rangle 7.$ Q.E.D.

PROOF: By $\langle 6\rangle 5$ and $\langle 6\rangle 6$

$\langle 5\rangle 4.$ $(p_1, n_1) \mapsto_{rr} (p_5, n_5)$

$\langle 6\rangle 1.$ $(p_1, n_1) \rightsquigarrow_{nr} (p_3, n_3)$

PROOF: By $\langle 4\rangle 1$

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

PROOF: By $\langle 6\rangle 1$, $\langle 5\rangle 2$ and Theorem 6

$\langle 5\rangle 5.$ $Q_5 \subseteq Q_1$

$\langle 6\rangle 1.$ $Q_3 \subseteq Q_1$

PROOF: By $\langle 4\rangle 1$

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

PROOF: By $\langle 6\rangle 1$ and $\langle 5\rangle 3$

$\langle 5\rangle 6.$ Q.E.D.

PROOF: By $\langle 5\rangle 4$ and $\langle 5\rangle 5$

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

PROOF: By $\langle 4\rangle 2$; $po_1$ is the $po$ we are looking for and $\langle I\rangle_{d_1}$ is the $S$ we are looking for.

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

PROOF: $\forall$-rule

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

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

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

PROOF: $\Rightarrow$-rule

□

**Monotonicity**

**Lemma 45 (Monotonicity of † w.r.t $\rightsquigarrow_{pg}$).** *Let $O$ and $O'$ be sets of p-obligations. Then*

$$O \rightsquigarrow_{pg} O' \Rightarrow \dagger O \rightsquigarrow_{pg} \dagger O'$$

PROOF.

⟨1⟩1. ASSUME: $O \rightsquigarrow_{pg} O'$
PROVE: $\dagger O \rightsquigarrow_{pg} \dagger O'$
⟨2⟩1. $\forall po \in \dagger O : 0 \notin \pi_2.po \Rightarrow \exists po' \in \dagger O' : po \rightsquigarrow_{pr} po'$
⟨3⟩1. ASSUME: $po \in \dagger O$
PROVE: $0 \notin \pi_2.po \Rightarrow \exists po' \in \dagger O' : po \rightsquigarrow_{pr} po'$
⟨4⟩1. ASSUME: $0 \notin \pi_2.po$
PROVE: $\exists po' \in \dagger O' : po \rightsquigarrow_{pr} po'$
⟨5⟩1. LET: $po_1 \in O$ such that $po = \dagger po_1$
PROOF: By assumption ⟨3⟩1
⟨5⟩2. $0 \notin \pi_2.po_1$
PROOF: By ⟨5⟩1 and assumption ⟨4⟩1
⟨5⟩3. LET: $po_1' \in O'$ such that $po_1 \rightsquigarrow_{pr} po_1'$
PROOF: By ⟨5⟩1, ⟨5⟩2 and assumption ⟨1⟩1
⟨5⟩4. $\dagger po_1 \rightsquigarrow_{pr} \dagger po_1'$
PROOF: By ⟨5⟩3 and Lemma 9
⟨5⟩5. $po \rightsquigarrow_{pr} \dagger po_1'$
PROOF: By ⟨5⟩4 and ⟨5⟩1
⟨5⟩6. $\dagger po_1' \in \dagger O'$
PROOF: By ⟨5⟩3
⟨5⟩7. Q.E.D.
PROOF: By ⟨5⟩5 and ⟨5⟩6; $\dagger po_1'$ is the $po'$ we are looking for
⟨4⟩2. Q.E.D.
PROOF: ⇒-rule
⟨3⟩2. Q.E.D.
PROOF: ∀-rule
⟨2⟩2. Q.E.D.
PROOF: By ⟨2⟩1
⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

**Theorem 21 (Monotonicity of refuse w.r.t $\rightsquigarrow_{pg}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![ \ d \ ]\!] \rightsquigarrow_{pg} [\![ \ d' \ ]\!] \Rightarrow [\![ \ \mathsf{refuse}\ d \ ]\!] \rightsquigarrow_{pg} [\![ \ \mathsf{refuse}\ d' \ ]\!]$$

PROOF.

This follows immediately from Lemma 45. Lemma 45 has been stated as a separate lemma to emphasize that the proof applies to all sets of p-obligations, and not only those that are the semantics of a sequence diagram.

□

**Theorem 22 (Non-monotonicity of palt w.r.t $\rightsquigarrow_{pg}$).** *Let $d_1, \ldots, d_n, d_1', \ldots, d_n'$ be sequence diagrams in $\mathcal{D}^p$. Furthermore, let $d = \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)$ and*

$d' = \mathsf{palt}(d'_1;Q'_1,\ldots,d'_n;Q'_n)$. *Then*

$$(\forall i \leq n : (\llbracket\ d_i\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d'_i\ \rrbracket \wedge Q'_i \subseteq Q_i)) \not\Rightarrow \llbracket\ d\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d'\ \rrbracket$$

PROOF. See the counter example given after Theorem 6 in [RHS07a]. □

**Lemma 46 (Monotonicity of † w.r.t $\rightsquigarrow_{prg}$).** *Let $O$ and $O'$ be sets of p-obligations. Then*

$$O \rightsquigarrow_{prg} O' \Rightarrow \dagger O \rightsquigarrow_{prg} \dagger O'$$

PROOF.

⟨1⟩1. ASSUME: $O \rightsquigarrow_{prg} O'$
  PROVE: $\dagger O \rightsquigarrow_{prg} \dagger O'$
 ⟨2⟩1. $\forall po \in \dagger O : 0 \notin \pi_2.po \Rightarrow \exists po' \in \dagger O' : po \rightsquigarrow_{prr} po'$
  ⟨3⟩1. ASSUME: $po \in \dagger O$
    PROVE: $0 \notin \pi_2.po \Rightarrow \exists po' \in \dagger O' : po \rightsquigarrow_{prr} po'$
   ⟨4⟩1. ASSUME: $0 \notin \pi_2.po$
     PROVE: $\exists po' \in \dagger O' : po \rightsquigarrow_{prr} po'$
    ⟨5⟩1. LET: $po_1 \in O$ such that $po = \dagger po_1$
     PROOF: By assumption ⟨3⟩1
    ⟨5⟩2. $0 \notin \pi_2.po_1$
     PROOF: By ⟨5⟩1 and assumption ⟨4⟩1
    ⟨5⟩3. LET: $po'_1 \in O'$ such that $po_1 \rightsquigarrow_{prr} po'_1$
     PROOF: By ⟨5⟩1, ⟨5⟩2 and assumption ⟨1⟩1
    ⟨5⟩4. $\dagger po_1 \rightsquigarrow_{prr} \dagger po'_1$
     ⟨6⟩1. $\pi_1.\dagger po_1 \rightsquigarrow_{rr} \pi_1.\dagger po'_1$
      ⟨7⟩1. $\pi_1.po_1 \rightsquigarrow_{rr} \pi_1.po'_1$
       PROOF: By ⟨5⟩3
      ⟨7⟩2. Q.E.D.
       PROOF: By ⟨7⟩1 and Theorem 8 in [RRS07]
     ⟨6⟩2. $\pi_2.\dagger po'_1 \subseteq \pi_2.\dagger po_1$
      ⟨7⟩1. $\pi_2.po'_1 \subseteq \pi_2.po_1$
       PROOF: By ⟨5⟩3
      ⟨7⟩2. Q.E.D.
       PROOF: By ⟨7⟩1
     ⟨6⟩3. Q.E.D.
      PROOF: By ⟨6⟩1 and ⟨6⟩2
    ⟨5⟩5. $po \rightsquigarrow_{prr} \dagger po'_1$
     PROOF: By ⟨5⟩4 and ⟨5⟩1
    ⟨5⟩6. $\dagger po'_1 \in \dagger O'$
     PROOF: By ⟨5⟩3
    ⟨5⟩7. Q.E.D.
     PROOF: By ⟨5⟩5 and ⟨5⟩6; $\dagger po'_1$ is the $po'$ we are looking for
   ⟨4⟩2. Q.E.D.
    PROOF: ⇒-rule
  ⟨3⟩2. Q.E.D.

Proof: $\forall$-rule

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

Proof: By $\langle 2\rangle 1$

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

Proof: $\Rightarrow$-rule

□

**Lemma 47 (Monotonicity of $\dagger$ w.r.t $\rightsquigarrow_{png}$).** *Let $O$ and $O'$ be sets of p-obligations. Then*

$$O \rightsquigarrow_{png} O' \Rightarrow \dagger O \rightsquigarrow_{png} \dagger O'$$

Proof. The proof is similar to the proof of Lemma 47; replace $\rightsquigarrow_{prg}$ with $\rightsquigarrow_{png}$, $\rightsquigarrow_{prr}$ with $\rightsquigarrow_{pnr}$, $\rightsquigarrow_{rr}$ with $\rightsquigarrow_{nr}$ and the reference to Theorem 8 in [RRS07] with a reference to Theorem 7. □

**Theorem 23 (Monotonicity of refuse w.r.t $\rightsquigarrow_{prg}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d\ ]\!] \rightsquigarrow_{prg} [\![\ d'\ ]\!] \Rightarrow [\![\ \mathsf{refuse}\ d\ ]\!] \rightsquigarrow_{prg} [\![\ \mathsf{refuse}\ d'\ ]\!]$$

Proof. This follows immediately from Lemma 46 □

**Lemma 48 (Monotonicity of $\succsim$ w.r.t $\rightsquigarrow_{prg}$.).** *Let $O_1, O_2, O_1', O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{prg} O_1' \wedge O_2 \rightsquigarrow_{prg} O_2' \Rightarrow O_1 \succsim O_2 \rightsquigarrow_{prg} O_1' \succsim O_2'$$

Proof.

$\langle 1\rangle 1.$ Assume: $O_1 \rightsquigarrow_{prg} O_1' \wedge O_2 \rightsquigarrow_{prg} O_2'$
Prove: $O_1 \succsim O_2 \rightsquigarrow_{prg} O_1' \succsim O_2'$

$\langle 2\rangle 1.$ $\forall po \in O_1 \succsim O_2 : 0 \notin \pi_2.po \Rightarrow \exists po' \in O_1' \succsim O_2' : po \rightsquigarrow_{prr} po'$

$\langle 3\rangle 1.$ Assume: $po \in O_1 \succsim O_2$
Prove: $0 \notin \pi_2.po \Rightarrow \exists po' \in O_1' \succsim O_2' : po \rightsquigarrow_{prr} po'$

$\langle 4\rangle 1.$ Assume: $0 \notin \pi_2.po$
Prove: $\exists po' \in O_1' \succsim O_2' : po \rightsquigarrow_{prr} po'$

$\langle 5\rangle 1.$ Let: $po_1 \in O_1, po_2 \in O_2$ such that $po = po_1 \succsim po_2$
Proof: By assumption $\langle 3\rangle 1$

$\langle 5\rangle 2.$ $0 \notin \pi_2.po_1 \wedge 0 \notin \pi_2.po_2$
Proof: By assumption $\langle 4\rangle 1$

$\langle 5\rangle 3.$ Let: $po_1' \in O_1', po_2' \in O_2'$ such that $po_1 \rightsquigarrow_{prr} po_1' \wedge po_2 \rightsquigarrow_{prr} po_2'$
Proof: By assumption $\langle 1\rangle 1$ and $\langle 5\rangle 2$

$\langle 5\rangle 4.$ $po_1' \succsim po_2' \in O_1' \succsim O_2'$
Proof: By $\langle 5\rangle 3$

$\langle 5\rangle 5.$ $po_1 \succsim po_2 \rightsquigarrow_{prr} po_1' \succsim po_2'$

$\langle 6\rangle 1.$ $\pi_1.(po_1 \succsim po_2) \rightsquigarrow_{rr} \pi_1.(po_1' \succsim po_2')$

$\langle 7\rangle 1.$ $\pi_1.(po_1 \succsim po_2) = (\pi_1.po_1) \succsim (\pi_1.po_2) \wedge \pi_1.(po_1' \succsim po_2') = (\pi_1.po_1') \succsim (\pi_1.po_2')$

Proof: By definition 50

$\langle 7\rangle 2.$ $\pi_1.po_1 \rightsquigarrow_{rr} \pi_1.po_1' \wedge \pi_1.po_2 \rightsquigarrow_{rr} \pi_1.po_2'$

Proof: By $\langle 5\rangle 3$

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

Proof: By $\langle 7\rangle 2$, Theorem 9 in [RRS07] and $\langle 7\rangle 1$

$\langle 6\rangle 2.$ $\pi_2.(po_1' \succsim po_2') \subseteq \pi_2.(po_1 \succsim po_2)$

$\langle 7\rangle 1.$ $\pi_2.(po_1' \succsim po_2') = Q_1' * Q_2' \wedge \pi_2.(po_2 \succsim po_2) = Q_1 * Q_2$

Proof: By definition 50

$\langle 7\rangle 2.$ $Q_1' \subseteq Q_1 \wedge Q_2' \subseteq Q_2$

Proof: By $\langle 5\rangle 3$

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

Proof: By $\langle 7\rangle 1$ and $\langle 7\rangle 2$

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

Proof: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$

$\langle 5\rangle 6.$ Q.E.D.

Proof: By $\langle 5\rangle 4$ and $\langle 5\rangle 5$; $po_1' \succsim po_2'$ is the $po'$ we are looking for

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

Proof: $\Rightarrow$-rule

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

Proof: $\forall$-rule

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

Proof: By $\langle 2\rangle 1$

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

Proof: $\Rightarrow$-rule

□

**Lemma 49 (Monotonicity of $\succsim$ w.r.t $\rightsquigarrow_{png}$).** *Let $O_1, O_2, O_1', O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{png} O_1' \wedge O_2 \rightsquigarrow_{png} O_2' \Rightarrow O_1 \succsim O_2 \rightsquigarrow_{png} O_1' \succsim O_2'$$

Proof. The proof is similar to the proof of Lemma 48, with the following replacements:

1. $\rightsquigarrow_{prg}$ is replaced with $\rightsquigarrow_{png}$
2. $\rightsquigarrow_{prr}$ is replaced with $\rightsquigarrow_{pnr}$
3. $\rightsquigarrow_{rr}$ is replaced with $\rightsquigarrow_{nr}$
4. The reference to Theorem 9 in [RRS07] is replaced with a reference to Theorem 8

**Lemma 50 (Monotonicity of $\parallel$ w.r.t $\rightsquigarrow_{png}$).** *Let $O_1, O_2, O_1', O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{png} O_1' \wedge O_2 \rightsquigarrow_{png} O_2' \Rightarrow O_1 \parallel O_2 \rightsquigarrow_{png} O_1' \parallel O_2'$$

Proof. The proof is similar to the proof of Lemma 48, with the following replacements:

1. $\rightsquigarrow_{prg}$ is replaced with $\rightsquigarrow_{png}$
2. $\rightsquigarrow_{prr}$ is replaced with $\rightsquigarrow_{pnr}$
3. $\rightsquigarrow_{rr}$ is replaced with $\rightsquigarrow_{nr}$
4. $\succsim$ is replaced with $\|$
5. The reference to definition 50 is replaced with a reference to definition 49
6. The reference to Theorem 9 in [RRS07] is replaced with a reference to Theorem 9

**Lemma 51 (Monotonicity of $\uplus$ w.r.t $\rightsquigarrow_{png}$).** *Let $O_1, O_2, O_1', O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{png} O_1' \wedge O_2 \rightsquigarrow_{png} O_2' \Rightarrow O_1 \uplus O_2 \rightsquigarrow_{png} O_1' \uplus O_2'$$

Proof. The proof is similar to the proof of Lemma 48, with the following replacements:

1. $\rightsquigarrow_{prg}$ is replaced with $\rightsquigarrow_{png}$
2. $\rightsquigarrow_{prr}$ is replaced with $\rightsquigarrow_{pnr}$
3. $\rightsquigarrow_{rr}$ is replaced with $\rightsquigarrow_{nr}$
4. $\succsim$ is replaced with $\uplus$
5. The reference to definition 50 is replaced with a reference to definition 51
6. The reference to Theorem 9 in [RRS07] is replaced with a reference to Theorem 10

**Theorem 24 (Monotonicity of seq w.r.t $\rightsquigarrow_{prg}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_2'\ \rrbracket \Rightarrow \llbracket\ d_1 \text{ seq } d_2\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_1' \text{ seq } d_2'\ \rrbracket$$

Proof. This follows immediately from Lemma 48

□

**Lemma 52 (Monotonicity of $\|$ w.r.t $\rightsquigarrow_{prg}$).** *Let $O_1, O_2, O_1', O_2'$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{prg} O_1' \wedge O_2 \rightsquigarrow_{prg} O_2' \Rightarrow O_1 \succsim O_2 \rightsquigarrow_{prg} O_1' \parallel O_2'$$

Proof. The proof is similar to the proof of Lemma 48; just replace $\succsim$ by $\|$, refer to Theorem 10 in [RRS07] instead of Theorem 9 in [RRS07] and definition 49 instead of definition 50.

□

**Theorem 25 (Monotonicity of par w.r.t $\rightsquigarrow_{prg}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_2'\ \rrbracket \Rightarrow \llbracket\ d_1 \text{ par } d_2\ \rrbracket \rightsquigarrow_{prg} \llbracket\ d_1' \text{ par } d_2'\ \rrbracket$$

Proof. This follows immediately from Lemma 52.

□

**Lemma 53 (Monotonicity of $\uplus$ w.r.t $\rightsquigarrow_{prg}$).** *Let $O_1, O_2, O'_1, O'_2$ be sets of p-obligations. Then*

$$O_1 \rightsquigarrow_{prg} O'_1 \wedge O_2 \rightsquigarrow_{prg} O'_2 \Rightarrow O_1 \uplus O_2 \rightsquigarrow_{prg} O'_1 \uplus O'_2$$

Proof. The proof is similar to the proof of Lemma 48; just replace $\succsim$ by $\uplus$, refer to Theorem 12 in [RRS07] instead of Theorem 9 in [RRS07] and definition 51 instead of definition 50.

□

**Theorem 26 (Monotonicity of $\mathsf{alt}$ w.r.t $\rightsquigarrow_{prg}$).** *Let $d_1$, $d_2$, $d'_1$ and $d'_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![ d_1 ]\!] \rightsquigarrow_{prg} [\![ d'_1 ]\!] \wedge [\![ d_2 ]\!] \rightsquigarrow_{prg} [\![ d'_2 ]\!] \Rightarrow [\![ d_1 \mathsf{~alt~} d_2 ]\!] \rightsquigarrow_{prg} [\![ d'_1 \mathsf{~alt~} d'_2 ]\!]$$

Proof. This follows immediately from Lemma 53

□

**Theorem 27 (Non-monotonicity of $\mathsf{palt}$ w.r.t $\rightsquigarrow_{prg}$).** *Let $d_1, \ldots, d_n, d'_1 \ldots, d'_n$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\begin{aligned}&(\forall i \leq n : ([\![ d_i ]\!] \rightsquigarrow_{prg} [\![ d'_i ]\!] \wedge Q'_i \subseteq Q_i)) \not\Rightarrow\\ &[\![ \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n) ]\!] \rightsquigarrow_{prg} [\![ \mathsf{palt}(d'_1;Q'_1, \ldots, d'_n;Q'_n) ]\!]\end{aligned}$$

Proof. To see this let

$$\begin{aligned} d_1 &= a\\ d_2 &= b\\ d'_2 &= b \mathsf{~alt~} (\mathsf{refuse~} a)\\ d &= \mathsf{palt}(d_1;\{0.5\}, d_2;\{0.5\})\\ d' &= \mathsf{palt}(d_1;\{0.5\}, d'_2;\{0.5\}) \end{aligned}$$

This means that

$$\begin{aligned} [\![ d_1 ]\!] &= \{((\{\langle a\rangle\}, \emptyset), \{1\})\}\\ [\![ d_2 ]\!] &= \{((\{\langle b\rangle\}, \emptyset), \{1\})\}\\ [\![ d'_2 ]\!] &= \{((\{\langle b\rangle\}, \{\langle a\rangle\}), \{1\})\}\\ [\![ d ]\!] &= \{((\{\langle a\rangle\}, \emptyset), \{0, 5\}), ((\{\langle b\rangle\}, \emptyset), \{0, 5\}), ((\emptyset, \emptyset), \{1\})\}\\ [\![ d' ]\!] &= \{((\{\langle a\rangle\}, \emptyset), \{0, 5\}), ((\{\langle b\rangle\}, \{\langle a\rangle\}), \{0, 5\}), ((\{\langle a\rangle\}, \emptyset), \{1\})\} \end{aligned}$$

which gives

$$\begin{aligned} [\![ d_1 ]\!] &\rightsquigarrow_{prg} [\![ d_1 ]\!]\\ [\![ d_2 ]\!] &\rightsquigarrow_{prg} [\![ d'_2 ]\!] \end{aligned}$$

But $[\![ d ]\!] \rightsquigarrow_{prg} [\![ d' ]\!]$ does not hold, because there is no p-obligation $po$ in $[\![ d' ]\!]$ such that $((\emptyset, \emptyset), \{1\}) \rightsquigarrow_{prr} po$.

**Theorem 28 (Monotonicity of $\mathsf{refuse}$ w.r.t $\rightsquigarrow_{pl}$).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![ d ]\!] \rightsquigarrow_{pl} [\![ d' ]\!] \Rightarrow [\![ \mathsf{refuse}\ d ]\!] \rightsquigarrow_{pl} [\![ \mathsf{refuse}\ d' ]\!]$$

Proof.

⟨1⟩1. Assume: $[\![ d ]\!] \rightsquigarrow_{pl} [\![ d' ]\!]$
Prove: $[\![ \mathsf{refuse}\ d ]\!] \rightsquigarrow_{pl} [\![ \mathsf{refuse}\ d' ]\!]$

⟨2⟩1. $[\![ \mathsf{refuse}\ d ]\!] \rightsquigarrow_{pg} [\![ \mathsf{refuse}\ d' ]\!]$

⟨3⟩1. $[\![ d ]\!] \rightsquigarrow_{pg} [\![ d' ]\!]$
Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.
Proof: By ⟨3⟩1 and Theorem 21

⟨2⟩2. $\forall po' \in [\![ \mathsf{refuse}\ d' ]\!] : \exists S \subseteq [\![ \mathsf{refuse}\ d' ]\!] : \exists po \in [\![ \mathsf{refuse}\ d ]\!] : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨3⟩1. Assume: $po' \in [\![ \mathsf{refuse}\ d' ]\!]$
Prove: $\exists S \subseteq [\![ \mathsf{refuse}\ d' ]\!] : \exists po \in [\![ \mathsf{refuse}\ d ]\!] : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨4⟩1. Let: $po'_1 \in [\![ d' ]\!]$ such that $po' = \dagger po'_1$
Proof: By assumption ⟨3⟩1

⟨4⟩2. Let: $po_1 \in [\![ d ]\!], S_1 \subseteq [\![ d' ]\!]$ such that $po'_1 \in S_1 \wedge po_1 \rightsquigarrow_{pr} \bar{\oplus} S_1$
Proof: By ⟨4⟩1 and assumption ⟨1⟩1

⟨4⟩3. $\dagger S_1 \subseteq [\![ \mathsf{refuse}\ d' ]\!]$
Proof: By ⟨4⟩2 ($S_1 \subseteq [\![ d' ]\!]$) and definition 48

⟨4⟩4. $\dagger po_1 \in [\![ \mathsf{refuse}\ d ]\!]$
Proof: By ⟨4⟩2 ($po_1 \in [\![ d ]\!]$) and definition 48

⟨4⟩5. $\dagger po_1 \rightsquigarrow_{pr} \bar{\oplus} \dagger S_1$

⟨5⟩1. $\dagger po_1 \rightsquigarrow_{pr} \dagger \bar{\oplus} S_1$
Proof: By ⟨4⟩2 ($po_1 \rightsquigarrow_{pr} \bar{\oplus} S_1$) and Lemma 9

⟨5⟩2. $\dagger \bar{\oplus} S_1 = \bar{\oplus} \dagger S_1$
Proof: By Lemma 8

⟨5⟩3. Q.E.D.
Proof: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩6. $po' \in \dagger S_1$
Proof: By ⟨4⟩1 ($po' = \dagger po'_1$) and ⟨4⟩2 ($po'_1 \in S_1$)

⟨4⟩7. Q.E.D.
Proof: By ⟨4⟩3, ⟨4⟩4, ⟨4⟩5 and ⟨4⟩6; $\dagger po_1$ is the $po$ we are looking for and $\dagger S_1$ is the $S$ we are looking for

⟨3⟩2. Q.E.D.
Proof: ∀-rule

⟨2⟩3. Q.E.D.
Proof: By ⟨2⟩1 and ⟨2⟩2

⟨1⟩2. Q.E.D.
Proof: ⇒-rule

□

**Theorem 29 (Monotonicity of $\mathsf{seq}$ w.r.t $\rightsquigarrow_{pl}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_2'\ \rrbracket \Rightarrow \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$$

Proof.

⟨1⟩1. Assume: $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_2'\ \rrbracket$
Prove: $\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$

⟨2⟩1. $\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$

⟨3⟩1. $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_2'\ \rrbracket$
Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.
Proof: By ⟨3⟩1 and Theorem 3 in [RHS07a]

⟨2⟩2. $\forall po' \in \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket : \exists S \subseteq \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket : \exists po \in \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨3⟩1. Assume: $po' \in \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$
Prove: $\exists S \subseteq \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket : \exists po \in \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨4⟩1. Let: $po_1 \in \llbracket\ d_1\ \rrbracket$ such that $po_1 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket$
$po_2 \in \llbracket\ d_2\ \rrbracket$ such that $po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_2\ \rrbracket$
Proof: By Lemma 11

⟨4⟩2. $po_1 \succsim po_2 \in \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket$
Proof: By ⟨4⟩1

⟨4⟩3. $po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket$

⟨5⟩1. $\pi_1.(po_1 \succsim po_2) \rightsquigarrow_r \oplus(\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket)$

⟨6⟩1. $po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \succsim \bar{\oplus}\llbracket\ d_2\ \rrbracket$
Proof: By ⟨4⟩1 and Lemma 3

⟨6⟩2. $\pi_1.(po_1 \succsim po_2) \rightsquigarrow_r \oplus\llbracket\ d_1\ \rrbracket \succsim \oplus\llbracket\ d_2\ \rrbracket$
Proof: By ⟨6⟩1

⟨6⟩3. $\oplus\llbracket\ d_1\ \rrbracket \succsim \oplus\llbracket\ d_2\ \rrbracket \rightsquigarrow_r \oplus(\llbracket\ d_1\ \rrbracket \succsim \llbracket\ d_2\ \rrbracket)$
Proof: By Lemma 4

⟨6⟩4. Q.E.D.
Proof: By ⟨6⟩2, ⟨6⟩3 and transitivity of $\rightsquigarrow_r$

⟨5⟩2. $\pi_2.\bar{\oplus}(\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket) \subseteq \pi_2.(po_1 \succsim po_2)$

⟨6⟩1. Q.E.D.
Proof: By ⟨4⟩1 and Lemma 18

⟨5⟩3. Q.E.D.
Proof: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩4. $\bar{\oplus}\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$

⟨5⟩1. $\oplus\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_r \oplus\llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$
Proof: By assumption ⟨1⟩1 and Lemma 40

⟨5⟩2. $\pi_2.\bar{\oplus}\llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket \subseteq \pi_2.\bar{\oplus}\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket$

⟨6⟩1. $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_2'\ \rrbracket$
Proof: By assumption ⟨1⟩1

⟨6⟩2. Q.E.D.
Proof: By ⟨6⟩1 and Lemma 42

⟨5⟩3. Q.E.D.

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

$\langle 4\rangle 5.$ $po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}[\![\ d_1' \ \mathsf{seq}\ d_2'\ ]\!]$

PROOF: By $\langle 4\rangle 3$, $\langle 4\rangle 4$ and transitivity of $\rightsquigarrow_{pr}$ (Lemma 1 in [RHS07a])

$\langle 4\rangle 6.$ Q.E.D.

PROOF: By $\langle 4\rangle 2$ and $\langle 4\rangle 5$; $po_1 \succsim po_2$ is the $po$ we are looking for and $[\![\ d_1' \ \mathsf{seq}\ d_2'\ ]\!]$ is the $S$ we are looking for

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

PROOF: $\forall$-rule

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

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

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

PROOF: $\Rightarrow$-rule

□

Note that $\pi_2.(\bar{\oplus}(S_1 \succsim S_2)) \subseteq \pi_2.(\bar{\oplus}S_1) * \pi_2.(\bar{\oplus}S_1)$ does not hold for all sets $S_1$ and $S_1$, as explained after Lemma 4. Therefore $po_1 \rightsquigarrow_{pr} \bar{\oplus}S_1 \wedge po_2 \rightsquigarrow_{pr} \bar{\oplus}S_2 \Rightarrow po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}(S_1 \succsim S_2)$ does not hold. This is the reason why the we have chosen a somewhat cumbersome proof strategy for Theorem 29.

**Theorem 30 (Monotonicity of $\mathsf{par}$ w.r.t $\rightsquigarrow_{pl}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{pl} [\![\ d_1'\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{pl} [\![\ d_2'\ ]\!] \Rightarrow [\![\ d_1\ \mathsf{par}\ d_2\ ]\!] \rightsquigarrow_{pl} [\![\ d_1'\ \mathsf{par}\ d_2'\ ]\!]$$

PROOF. The proof is similar to the proof of Theorem 29, with the following replacements:

1. $\mathsf{seq}$ is replaced with $\mathsf{par}$.
2. $\succsim$ is is replaced with $\|$.
3. Any reference to Theorem 3 in [RHS07a] is replaced by a reference to Theorem 4 in [RHS07a].
4. Any reference to Lemma 4 is replaced by a reference to Lemma 5.
5. Any reference to Lemma 40 is replaced by a reference to Lemma 41

□

**Theorem 31 (Monotonicity of $\mathsf{alt}$ w.r.t $\rightsquigarrow_{pl}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{pl} [\![\ d_1'\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{pl} [\![\ d_2'\ ]\!] \Rightarrow [\![\ d_1\ \mathsf{alt}\ d_2\ ]\!] \rightsquigarrow_{pl} [\![\ d_1'\ \mathsf{alt}\ d_2'\ ]\!]$$

PROOF. The proof is similar to the proof of Theorem 29, with the following replacements:

1. $\mathsf{seq}$ is replaced with $\mathsf{alt}$.
2. $\succsim$ is is replaced with $\uplus$.
3. Any reference to Theorem 3 in [RHS07a] is replaced by a reference to Theorem 5 in [RHS07a].
4. Any reference to Lemma 4 is replaced by a reference to Lemma 6.

5. Any reference to Lemma 40 is replaced by a reference to Lemma 19

□

**Theorem 32 (Monotonicity of** $\mathsf{palt}$ **w.r.t** $\rightsquigarrow_{pl}$**).** *Let* $d_1, \ldots, d_n, d'_1, \ldots, d'_n$ *be sequence diagrams in* $\mathcal{D}^p$*. Furthermore, let* $d = \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)$ *and* $d' = \mathsf{palt}(d'_1;Q'_1, \ldots, d'_n;Q'_n)$*. Then*

$$\forall i \leq n : \llbracket\ d_i\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d'_i\ \rrbracket \wedge Q'_i \subseteq Q_i \Rightarrow \llbracket\ d\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d'\ \rrbracket$$

PROOF.

⟨1⟩1. ASSUME: $\forall i \leq n : \llbracket\ d_i\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d'_i\ \rrbracket \wedge Q'_i \subseteq Q_i$
PROVE: $\llbracket\ d\ \rrbracket \rightsquigarrow_{pl} \llbracket\ d'\ \rrbracket$

⟨2⟩1. $\forall i \leq n : \oplus\llbracket\ d_i\ \rrbracket \rightsquigarrow_{r} \oplus\llbracket\ d'_i\ \rrbracket$
PROOF: By assumption ⟨1⟩1 and Lemma 1

⟨2⟩2. $\llbracket\ d\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d'\ \rrbracket$
PROOF: By assumption ⟨1⟩1, ⟨2⟩1 and Theorem 6 in [RHS07a]

⟨2⟩3. $\forall po' \in \llbracket\ d'\ \rrbracket : \exists S \subseteq \llbracket\ d'\ \rrbracket, po \in \llbracket\ d\ \rrbracket : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨3⟩1. ASSUME: $po' \in \llbracket\ d'\ \rrbracket$
PROVE: $\exists S \subseteq \llbracket\ d'\ \rrbracket, po \in \llbracket\ d\ \rrbracket : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨4⟩1. LET: $po_a \in \llbracket\ d\ \rrbracket$ such that $po_a \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d\ \rrbracket$
PROOF: By Lemma 11

⟨4⟩2. $po_a \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d'\ \rrbracket$

⟨5⟩1. $\pi_1.po_a \rightsquigarrow \oplus\llbracket\ d'\ \rrbracket$

⟨6⟩1. $\oplus\llbracket\ d\ \rrbracket = \oplus\bigcup_{i=1}^{n}\llbracket\ d_i\ \rrbracket \wedge \oplus\llbracket\ d'\ \rrbracket = \oplus\bigcup_{i=1}^{n}\llbracket\ d'_i\ \rrbracket$
PROOF: By definition 4 and definition 9

⟨6⟩2. $\oplus\llbracket\ d\ \rrbracket \rightsquigarrow_{r} \oplus\llbracket\ d'\ \rrbracket$
PROOF: By ⟨6⟩1, ⟨2⟩1 and Lemma 10

⟨6⟩3. $\pi_1.po_a \rightsquigarrow_{r} \oplus\llbracket\ d\ \rrbracket$
PROOF: By ⟨4⟩1

⟨6⟩4. Q.E.D.
PROOF: By ⟨6⟩3, ⟨6⟩2 and transitivity of $\rightsquigarrow_{r}$

⟨5⟩2. $\pi_2.\bar{\oplus}\llbracket\ d'\ \rrbracket \subseteq \pi_2.po_a$

⟨6⟩1. $\pi_2.\bar{\oplus}\llbracket\ d'\ \rrbracket \subseteq \pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket$
PROOF: By assumption ⟨1⟩1 and Lemma 21

⟨6⟩2. $\pi_2.\bar{\oplus}\llbracket\ d\ \rrbracket \subseteq \pi_2.po_a$
PROOF: By ⟨4⟩1

⟨6⟩3. Q.E.D.
PROOF: By ⟨6⟩1 and ⟨6⟩2

⟨5⟩3. Q.E.D.
PROOF: By ⟨5⟩1 and ⟨5⟩2

⟨4⟩3. Q.E.D.
PROOF: By ⟨4⟩1 and ⟨4⟩2; $po_a$ is the $po$ we are looking for and $\llbracket\ d'\ \rrbracket$ is the $S$ we are looking for.

⟨3⟩2. Q.E.D.
PROOF: $\forall$-rule

⟨2⟩4. Q.E.D.

Proof: By ⟨2⟩2, ⟨2⟩3 and definition 25

⟨1⟩2. Q.E.D.

Proof: ⇒-rule

□

**Lemma 54 (Monotonicity of † w.r.t $\rightsquigarrow_{prl}$).** *Let* $O, O'$ *be sets of p-obligations. Then*

$$O \rightsquigarrow_{prl} O' \Rightarrow \dagger O \rightsquigarrow_{prl} \dagger O'$$

Proof.

⟨1⟩1. Assume: $O \rightsquigarrow_{prl} O'$
Prove: $\dagger O \rightsquigarrow_{prl} \dagger O'$

⟨2⟩1. $\dagger O \rightsquigarrow_{prg} \dagger O'$

⟨3⟩1. $O \rightsquigarrow_{prg} O'$

Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.

Proof: By ⟨3⟩1 and Lemma 46

⟨2⟩2. $\forall po' \in \dagger O' : \exists S \subseteq \dagger O' : \exists po \in \dagger O : po' \in S \wedge po \rightsquigarrow_{prr} \bar{\oplus} S$

⟨3⟩1. Assume: $po'_1 \in \dagger O'$
Prove: $\exists S \subseteq \dagger O' : \exists po \in \dagger O : po'_1 \in S \wedge po \rightsquigarrow_{prr} \bar{\oplus} S$

⟨4⟩1. Let: $po'_2 \in O'$ such that $po'_1 = \dagger po'_2$

Proof: By assumption ⟨3⟩1

⟨4⟩2. Let: $S_2 \subseteq O', po_2 \in O$ such that $po'_2 \in S_2 \wedge po_2 \rightsquigarrow_{prr} \bar{\oplus} S_2$

Proof: By ⟨4⟩1 and assumption ⟨1⟩1

⟨4⟩3. $\dagger S_2 \subseteq \dagger O' \wedge \dagger po_2 \in \dagger O$

Proof: By ⟨4⟩2

⟨4⟩4. $po'_1 \in \dagger S_2$

Proof: By ⟨4⟩2 and ⟨4⟩1

⟨4⟩5. $\dagger po_2 \rightsquigarrow_{prr} \bar{\oplus} \dagger S_2$

⟨5⟩1. $\dagger po_2 \rightsquigarrow_{pr} \dagger \bar{\oplus} S_2$

Proof: By ⟨4⟩2 and Lemma 9

⟨5⟩2. $\pi_1.\dagger \bar{\oplus} S_2 \subseteq \pi_1.\dagger po_2$

Proof: By definition 52 ($\pi_1.\dagger \bar{\oplus} S_2 = \pi_1.\dagger po_2 = \emptyset$)

⟨5⟩3. $\dagger po_2 \rightsquigarrow_{prr} \dagger \bar{\oplus} S_2$

Proof: By ⟨5⟩1 and ⟨5⟩2

⟨5⟩4. Q.E.D.

Proof: By ⟨5⟩3 and Lemma 8

⟨4⟩6. Q.E.D.

Proof: By ⟨4⟩3, ⟨4⟩4 and ⟨4⟩5; $\dagger S_2$ is the $S$ we are looking for and $\dagger po_2$ is the *po* we are looking for.

⟨3⟩2. Q.E.D.

Proof: ∀-rule

⟨2⟩3. Q.E.D.

Proof: By ⟨2⟩1 and ⟨2⟩2

⟨1⟩2. Q.E.D.

Proof: ⇒-rule

□

**Theorem 33 (Monotonicity of** $\mathsf{refuse}$ **w.r.t** $\rightsquigarrow_{prl}$**).** *Let* $d \in \mathcal{D}^p$*. Then*

$$[\![\ d\ ]\!] \rightsquigarrow_{prl} [\![\ d'\ ]\!] \Rightarrow [\![\ \mathsf{refuse}\ d\ ]\!] \rightsquigarrow_{prl} [\![\ \mathsf{refuse}\ d'\ ]\!]$$

Proof. This follows immediately from Lemma 54 □

**Theorem 34 (Non-monotonicity of** $\mathsf{seq}$ **w.r.t** $\rightsquigarrow_{prl}$**).** *Let* $d_1, d_2, d_1', d_2'$ *be sequence diagrams in* $\mathcal{D}^p$*. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{prl} [\![\ d_1'\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d_2'\ ]\!] \not\Rightarrow [\![\ d_1\ \mathsf{seq}\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d_1'\ \mathsf{seq}\ d_2'\ ]\!]$$

Proof. To see this, let

$$\begin{aligned}
&[\![\ d_1\ ]\!] = \{((\emptyset, \{\langle ab\rangle\}), \{1\})\}\\
&[\![\ d_2\ ]\!] = \{((\emptyset, \{\langle c\rangle\}), \{1\})\}\\
&[\![\ d_1'\ ]\!] = \{((\{\langle a\rangle\}, \{\langle ab\rangle\}), \{0.4\}), ((\{\langle x\rangle\}, \{\langle ab\rangle\}), \{0.6\}), ((\emptyset, \{\langle ab\rangle\}), \{1\})\}\\
&[\![\ d_2'\ ]\!] = \{((\{\langle bc\rangle\}, \{\langle c\rangle\}), \{0.3\}), ((\{\langle y\rangle\}, \{\langle c\rangle\}), \{0.7\}), ((\emptyset, \{\langle c\rangle\}), \{1\})\}
\end{aligned}$$

There exists syntactically correct sequence diagrams with the given semantics; $d_1'$ and $d_2'$ will have a binary $\mathsf{palt}$ as the outermost operand. From the above we get

$$\begin{aligned}
\bar{\oplus}[\![\ d_1'\ ]\!] &= ((\emptyset, \{\langle ab\rangle\}), \{1\})\\
\bar{\oplus}[\![\ d_2'\ ]\!] &= ((\emptyset, \{\langle c\rangle\}), \{1\})\\
[\![\ d_1\ \mathsf{seq}\ d_2\ ]\!] &= \{((\emptyset, \{\langle abc\rangle\}), \{1\})\}\\
[\![\ d_1'\ \mathsf{seq}\ d_2'\ ]\!] &= \{\ ((\{\langle abc\rangle\}, \{\langle ac\rangle, \langle abc\rangle, \langle abbc\rangle\}), \{0.12\}),\\
&\qquad ((\{\langle ay\rangle\}, \{\langle ac\rangle, \langle abc\rangle, \langle aby\rangle\}), \{0.28\}),\\
&\qquad ((\emptyset, \{\langle ac\rangle, \langle abc\rangle\}), \{0.4\}),\\
&\qquad ((\{\langle xbc\rangle\}, \{\langle xc\rangle, \langle abc\rangle, \langle abbc\rangle\}), \{0.18\}),\\
&\qquad ((\{\langle xy\rangle\}, \{\langle xc\rangle, \langle abc\rangle, \langle aby\rangle\}), \{0.42\}),\\
&\qquad ((\emptyset, \{\langle xc\rangle, \langle abc\rangle\}), \{0.6\}),\\
&\qquad ((\emptyset, \{\langle abc\rangle, \langle abbc\rangle\}), \{0.3\}),\\
&\qquad ((\emptyset, \{\langle abc\rangle, \langle aby\rangle\}), \{0.7\}),\\
&\qquad ((\emptyset, \{\langle abc\rangle\}), \{1\})\ \}\\
\bar{\oplus}[\![\ d_1'\ \mathsf{seq}\ d_2'\ ]\!] &= ((\{\langle abc\rangle\}, \{\langle abc\rangle\}), \{1\})
\end{aligned}$$

$[\![\ d_1\ ]\!] \rightsquigarrow_{prl} [\![\ d_1'\ ]\!]$ holds since $((\emptyset, \{\langle ab\rangle\}), \{1\}) \rightsquigarrow_{prr} ((\emptyset, \{\langle ab\rangle\}), \{1\})$; this ensures both that the only p-obligation in $[\![\ d_1\ ]\!]$ is represented in $[\![\ d_1'\ ]\!]$ and that each p-obligation in $[\![\ d_1'\ ]\!]$ is a member of a subset $S$ of $[\![\ d_1'\ ]\!]$ such that $\bar{\oplus}S$ is represented in $[\![\ d_1\ ]\!]$. For similar reasons $[\![\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d_2'\ ]\!]$ holds. But $[\![\ d_1\ \mathsf{seq}\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d_1'\ \mathsf{seq}\ d_2'\ ]\!]$ does not hold, since any subset of $[\![\ d_1'\ \mathsf{seq}\ d_2'\ ]\!]$ that contains $((\{\langle abc\rangle\}, \{\langle ac\rangle, \langle abc\rangle, \langle abbc\rangle\}), \{0.12\})$ will have $\langle abc\rangle$ as a positive trace. This trace is not positive in the only p-obligation in $[\![\ d_1\ \mathsf{seq}\ d_2\ ]\!]$.

The specifications in the above counterexample is not implementable according to $\mapsto_{prl}$, since we have p-obligations with no positive traces. But this could easily be fixed by adding new positive traces consisting only of new events to all p-obligations. Note also that $\langle abc \rangle$ is both positive and negative in $((\{\langle abc \rangle\}, \{\langle ac \rangle, \langle abc \rangle, \langle abbc \rangle\}), \{0.12\})$.

□

**Theorem 35 (Non-monotonicity of** $\mathsf{par}$ **w.r.t** $\rightsquigarrow_{prl}$**).** *Let* $d_1, d_2, d'_1, d'_2$ *be sequence diagrams in* $\mathcal{D}^p$*. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{prl} [\![\ d'_1\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d'_2\ ]\!] \not\Rightarrow [\![\ d_1 \text{ par } d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d'_1 \text{ par } d'_2\ ]\!]$$

Proof. The counterexample is similar to for Theorem 34

□

**Theorem 36 (Non-monotonicity of** $\mathsf{alt}$ **w.r.t** $\rightsquigarrow_{prl}$**).** *Let* $d_1, d_2, d'_1, d'_2$ *be sequence diagrams in* $\mathcal{D}^p$*. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{prl} [\![\ d'_1\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d'_2\ ]\!] \not\Rightarrow [\![\ d_1 \text{ alt } d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d'_1 \text{ alt } d'_2\ ]\!]$$

Proof. To see this, let

$$[\![\ d_1\ ]\!] = \{((\{\langle a \rangle, \langle b \rangle\}, \emptyset), \{1\})\}$$
$$[\![\ d'_1\ ]\!] = \{((\{\langle a \rangle, \langle d \rangle\}, \{\langle b \rangle\}), \{0.5\}), ((\{\langle b \rangle\}, \{\langle a \rangle\}), \{0.5\}), ((\{\langle a \rangle, \langle b \rangle\}, \emptyset), \{1\})\}$$
$$[\![\ d_2\ ]\!] = \{((\{\langle c \rangle\}, \{\langle d \rangle\}), \{1\})\}$$
$$[\![\ d'_2\ ]\!] = [\![\ d_2\ ]\!]$$

There exists syntactically correct sequence diagrams with the given semantics; $d'_1$ has a binary $\mathsf{palt}$ as the outermost operand. From the above we get

$$\begin{aligned}
[\![\ d_1 \text{ alt } d_2\ ]\!] &= \{((\{\langle a \rangle, \langle b \rangle, \langle c \rangle\}, \{\langle d \rangle\}), \{1\})\} \\
[\![\ d'_1 \text{ alt } d'_2\ ]\!] &= \{((\{\langle a \rangle, \langle c \rangle, \langle d \rangle\}, \{\langle b \rangle, \langle d \rangle\}), \{0.5\}), \\
&\qquad ((\{\langle b \rangle, \langle c \rangle\}, \{\langle a \rangle, \langle d \rangle\}), \{0.5\}), \\
&\qquad ((\{\langle a \rangle, \langle b \rangle, \langle c \rangle\}, \{\langle d \rangle\}), \{1\})\}
\end{aligned}$$

$[\![\ d_1\ ]\!] \rightsquigarrow_{prl} [\![\ d'_1\ ]\!]$ holds since $((\{\langle a \rangle, \langle b \rangle\}, \emptyset), \{1\}) \rightsquigarrow_{prr} ((\{\langle a \rangle, \langle b \rangle\}, \emptyset), \{1\})$; this ensures both that the only p-obligation in $[\![\ d_1\ ]\!]$ is represented in $[\![\ d'_1\ ]\!]$ and that each p-obligation in $[\![\ d'_1\ ]\!]$ is a member of a subset $S$ of $[\![\ d'_1\ ]\!]$ such that $\bar{\oplus} S$ is represented in $[\![\ d_1\ ]\!]$. $[\![\ d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d'_2\ ]\!]$ holds trivially since $[\![\ d_2\ ]\!] = [\![\ d'_2\ ]\!]$. But $[\![\ d_1 \text{ alt } d_2\ ]\!] \rightsquigarrow_{prl} [\![\ d'_1 \text{ alt } d'_2\ ]\!]$ does not hold, since the trace $\langle d \rangle$ will be positive in $\bar{\oplus} S$ for any subset $S$ of $[\![\ d'_1 \text{ alt } d'_2\ ]\!]$ that contains $((\{\langle a \rangle, \langle c \rangle, \langle d \rangle\}, \{\langle b \rangle, \langle d \rangle\}), \{0.5\})$, and $\langle d \rangle$ is not positive in the only p-obligation in $[\![\ d_1 \text{ alt } d_2\ ]\!]$.

□

**Theorem 37 (Non-monotonicity of** $\mathsf{palt}$ **w.r.t** $\rightsquigarrow_{prl}$**).** *Let* $d_1, \ldots, d_n, d'_1, \ldots, d'_n$ *be sequenced diagrams in* $\mathcal{D}^p$*. Then*

$$\begin{aligned}
&\forall i \leq n : [\![\ d_i\ ]\!] \rightsquigarrow_{prl} [\![\ d'_i\ ]\!] \wedge Q'_i \subseteq Q_i \not\Rightarrow \\
&\quad [\![\ \text{palt}(d_1;Q_1, \ldots, d_n;Q_n)\ ]\!] \rightsquigarrow_{prl} [\![\ \text{palt}(d'_1;Q'_1, \ldots, d'_n;Q'_n)\ ]\!]
\end{aligned}$$

Proof. The counter example is the same as for Theorem 27; just replace $\rightsquigarrow_{prg}$ with $\rightsquigarrow_{prl}$.

□

**Theorem 38 (Monotonicity of $\mathsf{refuse}$ w.r.t $\rightsquigarrow_{png}$).** *Let $d \in \mathcal{D}^p$. Then*

$$[\![\ d\ ]\!] \rightsquigarrow_{png} [\![\ d'\ ]\!] \Rightarrow [\![\ \mathsf{refuse}\ d\ ]\!] \rightsquigarrow_{png} [\![\ \mathsf{refuse}\ d'\ ]\!]$$

Proof. This follows immediately from Lemma 47 □

**Theorem 39 (Monotonicity of $\mathsf{seq}$ w.r.t $\rightsquigarrow_{png}$).** *Let $d_1$, $d_2$, $d'_1$ and $d'_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{png} [\![\ d'_1\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{png} [\![\ d'_2\ ]\!] \Rightarrow [\![\ d_1\ \mathsf{seq}\ d_2\ ]\!] \rightsquigarrow_{png} [\![\ d'_1\ \mathsf{seq}\ d'_2\ ]\!]$$

Proof. This follows immediately from Lemma 49 □

**Theorem 40 (Monotonicity of $\mathsf{par}$ w.r.t $\rightsquigarrow_{png}$).** *Let $d_1$, $d_2$, $d'_1$ and $d'_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{png} [\![\ d'_1\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{png} [\![\ d'_2\ ]\!] \Rightarrow [\![\ d_1\ \mathsf{par}\ d_2\ ]\!] \rightsquigarrow_{png} [\![\ d'_1\ \mathsf{par}\ d'_2\ ]\!]$$

Proof. This follows immediately from Lemma 50 □

**Theorem 41 (Monotonicity of $\mathsf{alt}$ w.r.t $\rightsquigarrow_{png}$).** *Let $d_1$, $d_2$, $d'_1$ and $d'_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$[\![\ d_1\ ]\!] \rightsquigarrow_{png} [\![\ d'_1\ ]\!] \wedge [\![\ d_2\ ]\!] \rightsquigarrow_{png} [\![\ d'_2\ ]\!] \Rightarrow [\![\ d_1\ \mathsf{alt}\ d_2\ ]\!] \rightsquigarrow_{png} [\![\ d'_1\ \mathsf{alt}\ d'_2\ ]\!]$$

Proof. This follows immediately from Lemma 51 □

**Theorem 42 (Non-monotonicity of $\mathsf{palt}$ w.r.t $\rightsquigarrow_{png}$).** *Let $d_1, \ldots, d_n, d'_1, \ldots, d'_n$ be sequence diagrams in $\mathcal{D}^p$. Furthermore, let $d = \mathsf{palt}(d_1;Q_1, \ldots, d_n;Q_n)$ and $d' = \mathsf{palt}(d'_1;Q'_1, \ldots, d'_n;Q'_n)$. Then*

$$\forall i \leq n : [\![\ d_i\ ]\!] \rightsquigarrow_{png} [\![\ d'_i\ ]\!] \wedge Q'_i \subseteq Q_i \not\Rightarrow [\![\ d\ ]\!] \rightsquigarrow_{png} [\![\ d'\ ]\!]$$

Proof. See the counter example given after Theorem 6 in [RHS07a]. □

**Theorem 43 (Monotonicity of $\mathsf{refuse}$ w.r.t $\rightsquigarrow_{pnl}$).** *Let $d \in \mathcal{D}^p$. Then*

$$[\![\ d\ ]\!] \rightsquigarrow_{pnl} [\![\ d'\ ]\!] \Rightarrow [\![\ \mathsf{refuse}\ d\ ]\!] \rightsquigarrow_{pnl} [\![\ \mathsf{refuse}\ d'\ ]\!]$$

Proof. The proof is similar to the proof of Theorem 28, with the following replacements:

1. $\rightsquigarrow_{pg}$ is replaced by $\rightsquigarrow_{png}$
2. $\rightsquigarrow_{pl}$ is replaced by $\rightsquigarrow_{pnl}$
3. $\rightsquigarrow_{pr}$ is replaced by $\rightsquigarrow_{pnr}$
4. The reference to Theorem 21 is replaced by a reference to Theorem 38
5. The reference to Lemma 9 is replaced by a reference to Lemma 14

$\square$

**Theorem 44 (Monotonicity of $\mathsf{seq}$ w.r.t $\rightsquigarrow_{pnl}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_2'\ \rrbracket \Rightarrow \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$$

Proof.

⟨1⟩1. Assume: $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_2'\ \rrbracket$
Prove: $\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$

⟨2⟩1. $\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket \rightsquigarrow_{png} \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$

⟨3⟩1. $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{png} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{png} \llbracket\ d_2'\ \rrbracket$
Proof: By assumption ⟨1⟩1

⟨3⟩2. Q.E.D.
Proof: By ⟨3⟩1 and Theorem 39

⟨2⟩2. $\forall po' \in \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket : \exists S \subseteq \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket : \exists po \in \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket :$
$po' \in S \wedge po \rightsquigarrow_{pnr} \bar{\oplus} S$

⟨3⟩1. Assume: $po' \in \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket$
Prove: $\exists S \subseteq \llbracket\ d_1'\ \mathsf{seq}\ d_2'\ \rrbracket : \exists po \in \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket :$
$po' \in S \wedge po \rightsquigarrow_{pnr} \bar{\oplus} S$

⟨4⟩1. Let: $po_1 \in \llbracket\ d_1\ \rrbracket$ such that $po_1 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_1\ \rrbracket$
$po_2 \in \llbracket\ d_2\ \rrbracket$ such that $po_2 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_2\ \rrbracket$
Proof: By Lemma 12

⟨4⟩2. $po_1 \succsim po_2 \in \llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket$
Proof: By ⟨4⟩1

⟨4⟩3. $po_1 \succsim po_2 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket$

⟨5⟩1. $\pi_1.(po_1 \succsim po_2) \rightsquigarrow_r \oplus(\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket)$

⟨6⟩1. $po_1 \succsim po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \succsim \bar{\oplus}\llbracket\ d_2\ \rrbracket$
Proof: By ⟨4⟩1 and Lemma 3

⟨6⟩2. $\pi_1.(po_1 \succsim po_2) \rightsquigarrow_r \oplus\llbracket\ d_1\ \rrbracket \succsim \oplus\llbracket\ d_2\ \rrbracket$
Proof: By ⟨6⟩1

⟨6⟩3. $\oplus\llbracket\ d_1\ \rrbracket \succsim \oplus\llbracket\ d_2\ \rrbracket \rightsquigarrow_r \oplus(\llbracket\ d_1\ \rrbracket \succsim \llbracket\ d_2\ \rrbracket)$
Proof: By Lemma 4

⟨6⟩4. Q.E.D.
Proof: By ⟨6⟩2, ⟨6⟩3 and transitivity of $\rightsquigarrow_r$

⟨5⟩2. Let: $po'' = po_1 \succsim po_2$
$po''' = \bar{\oplus}\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket$

⟨5⟩3. $p'' \cup n'' = p''' \cup n'''$

⟨6⟩1. $p'' \cup n'' \subseteq p''' \cup n'''$
Proof: By ⟨5⟩1

⟨6⟩2. $p''' \cup n''' \subseteq p'' \cup n''$
Proof: By ⟨4⟩2 and Lemma 25

⟨6⟩3. Q.E.D.
Proof: By ⟨6⟩1 og ⟨6⟩2

⟨5⟩4. $\pi_2.\bar{\oplus}(\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket) \subseteq \pi_2.(po_1 \succsim po_2)$

⟨6⟩1. $po_1 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1\ \rrbracket \wedge po_2 \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_2\ \rrbracket$

PROOF: By $\langle 4\rangle 1$

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

PROOF: By $\langle 6\rangle 1$ and Lemma 18

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

PROOF: By $\langle 5\rangle 1$, $\langle 5\rangle 3$ and $\langle 5\rangle 4$

$\langle 4\rangle 4.$ $\bar{\oplus}\llbracket\ d_1 \textsf{ seq } d_2\ \rrbracket \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket$

$\langle 5\rangle 1.$ $\oplus\llbracket\ d_1 \textsf{ seq } d_2\ \rrbracket \rightsquigarrow_{r} \oplus\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket$

PROOF: By assumption $\langle 1\rangle 1$ and Lemma 40

$\langle 5\rangle 2.$ $\pi_2.\bar{\oplus}\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket \subseteq \pi_2.\bar{\oplus}\llbracket\ d_1 \textsf{ seq } d_2\ \rrbracket$

$\langle 6\rangle 1.$ $\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pg} \llbracket\ d_2'\ \rrbracket$

PROOF: By $\langle 1\rangle 1$

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

PROOF: By $\langle 6\rangle 1$ and Lemma 42

$\langle 5\rangle 3.$ $\bar{\oplus}\llbracket\ d_1 \textsf{ seq } d_2\ \rrbracket \rightsquigarrow_{pr} \bar{\oplus}\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket$

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

$\langle 5\rangle 4.$ LET: $po'' = \bar{\oplus}\llbracket\ d_1 \textsf{ seq } d_2\ \rrbracket$
$po''' = \bar{\oplus}\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket$

$\langle 5\rangle 5.$ $p'' \cup n'' = p''' \cup n'''$

PROOF: By assumption $\langle 1\rangle 1$ and Lemma 22

$\langle 5\rangle 6.$ Q.E.D.

PROOF: By $\langle 5\rangle 3$ and $\langle 5\rangle 5$

$\langle 4\rangle 5.$ $po_1 \succsim po_2 \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket$

PROOF: By $\langle 4\rangle 3$, $\langle 4\rangle 4$ and Lemma 26

$\langle 4\rangle 6.$ Q.E.D.

PROOF: By $\langle 4\rangle 2$ and $\langle 4\rangle 5$; $po_1 \succsim po_2$ is the $po$ we are looking for and $\llbracket\ d_1' \textsf{ seq } d_2'\ \rrbracket$ is the $S$ we are looking for

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

PROOF: $\forall$-rule

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

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

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

PROOF: $\Rightarrow$-rule

□

**Theorem 45 (Monotonicity of par w.r.t $\rightsquigarrow_{pnl}$).** *Let $d_1$, $d_2$, $d_1'$ and $d_2'$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_1'\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_2'\ \rrbracket \Rightarrow \llbracket\ d_1 \textsf{ par } d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d_1' \textsf{ par } d_2'\ \rrbracket$$

PROOF. The proof is similar to the proof of Theorem 44, with the following replacements:

1. seq is replaced by par
2. $\succsim$ is replaced by $\|$
3. The reference to Lemma 4 is replaced by a reference to Lemma 5
4. The reference to Lemma 40 is replaced by a reference to Lemma 41
5. The reference to Lemma 22 is replaced by a reference to Lemma 23

6. The reference to Theorem 39 is replaced by a reference to Theorem 40

□

**Theorem 46 (Monotonicity of $\mathsf{alt}$ w.r.t $\rightsquigarrow_{pnl}$).** *Let $d_1$, $d_2$, $d'_1$ and $d'_2$ be sequence diagrams in $\mathcal{D}^p$. Then*

$$\llbracket\ d_1\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'_1\ \rrbracket \wedge \llbracket\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'_2\ \rrbracket \Rightarrow \llbracket\ d_1 \ \mathsf{alt}\ d_2\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'_1 \ \mathsf{alt}\ d'_2\ \rrbracket$$

Proof. The proof is similar to the proof of Theorem 44, with the following replacements:

1. $\mathsf{seq}$ is replaced by $\mathsf{alt}$
2. $\succsim$ is replaced by $\uplus$
3. The reference to Lemma 4 is replaced by a reference to Lemma 6
4. The reference to Lemma 40 is replaced by a reference to Lemma 19
5. The reference to Lemma 22 is replaced by a reference to Lemma 24
6. The reference to Theorem 39 is replaced by a reference to Theorem 41

□

**Theorem 47 (Monotonicity of $\mathsf{palt}$ w.r.t $\rightsquigarrow_{pnl}$).** *Let $d_1,\ldots,d_n,d'_1,\ldots,d'_n$ be sequence diagrams in $\mathcal{D}^p$. Furthermore, let $d = \mathsf{palt}(d_1;Q_1,\ldots,d_n;Q_n)$ and $d' = \mathsf{palt}(d'_1;Q'_1,\ldots,d'_n;Q'_n)$. Then*

$$\forall i \leq n : \llbracket\ d_i\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'_i\ \rrbracket \wedge Q'_i \subseteq Q_i \Rightarrow \llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'\ \rrbracket$$

Proof.

⟨1⟩1. Assume: $\forall i \leq n : \llbracket\ d_i\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'_i\ \rrbracket \wedge Q'_i \subseteq Q_i$
Prove: $\llbracket\ d\ \rrbracket \rightsquigarrow_{pnl} \llbracket\ d'\ \rrbracket$

⟨2⟩1. $\forall i \leq n : \oplus\llbracket\ d_i\ \rrbracket \rightsquigarrow_{nr} \oplus\llbracket\ d'_i\ \rrbracket$
Proof: By the assumption and Lemma 13

⟨2⟩2. $\llbracket\ d\ \rrbracket \rightsquigarrow_{png} \llbracket\ d'\ \rrbracket$

⟨3⟩1. $\forall po \in \llbracket\ d\ \rrbracket : 0 \notin \pi_2.po \Rightarrow \exists po' \in \llbracket\ d'\ \rrbracket : po \rightsquigarrow_{pnr} po'$

⟨4⟩1. Assume: $po_a \in \llbracket\ d\ \rrbracket$
Prove: $0 \notin \pi_2.po_a \Rightarrow \exists po' \in \llbracket\ d'\ \rrbracket : po_a \rightsquigarrow_{pnr} po'$

⟨5⟩1. Assume: $0 \notin \pi_2.po_a$
Prove: $\exists po' \in \llbracket\ d'\ \rrbracket : po_a \rightsquigarrow_{pnr} po'$

⟨6⟩1. Case: $po_a \in \{(\oplus \bigcup\limits_{i\in N}\{po_i\}, \sum\limits_{i\in N} \pi_2.po_i) \mid N \subseteq \{1,\ldots,n\} \wedge N \neq \emptyset \wedge \forall i \in N : po_i \in \llbracket\ d_i;Q_i\ \rrbracket\}$

⟨7⟩1. Let: $N \subseteq \{1,\ldots,n\}, po_i \in \llbracket\ d_i;Q_i\ \rrbracket$ for each $i \leq n$ such that $N \neq \emptyset \wedge po_a = (\oplus \bigcup_{i\in N}\{po_i\}, \sum_{i\in N} \pi_2.po_i)$
Proof: By assumption ⟨6⟩1

⟨7⟩2. Let: $po'_i \in \llbracket\ d'_i;Q'_i\ \rrbracket$ such that $po_i \rightsquigarrow_{pnr} po'_i$ for all $i \in N$
Proof: By the overall assumption

⟨7⟩3. $(\oplus \bigcup_{i\in N}\{po_i\}, \sum_{i\in N} \pi_2.po_i) \rightsquigarrow_{pnr} (\oplus \bigcup_{i\in N}\{po'_i\}, \sum_{i\in N} \pi_2.po'_i)$

⟨8⟩1. $(\oplus \bigcup_{i\in N}\{po_i\}, \sum_{i\in N} \pi_2.po_i) \rightsquigarrow_{pr} (\oplus \bigcup_{i\in N}\{po'_i\}, \sum_{i\in N} \pi_2.po'_i)$

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and Lemma 6 in [RHS07a]

$\langle 8\rangle 2.$ LET: $(p'', n'') = \oplus \bigcup_{i \in N}\{po_i\}$
$(p''', n''') = \oplus \bigcup_{i \in N}\{po'_i\}$

$\langle 8\rangle 3.$ $\forall i \in N : p_i \cup n_i = p'_i \cup n'_i$

PROOF: By $\langle 7\rangle 2$

$\langle 8\rangle 4.$ $p'' \cup n'' = p''' \cup n'''$

PROOF: By $\langle 8\rangle 3$ and definition 4

$\langle 8\rangle 5.$ Q.E.D.

PROOF: By $\langle 8\rangle 1$ and $\langle 8\rangle 4$

$\langle 7\rangle 4.$ $(\oplus \bigcup_{i \in N}\{po'_i\}, \sum_{i \in N} \pi_2.po'_i) \in \llbracket\ d'\ \rrbracket$

PROOF: By definition 9

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

PROOF: By $\langle 7\rangle 3$ and $\langle 7\rangle 4$; $(\oplus \bigcup_{i \in N}\{po'_i\}, \sum_{i \in N} \pi_2.po'_i)$ is the $po'$ we are looking for.

$\langle 6\rangle 2.$ CASE: $po_a = (\oplus \bigcup_{i=1}^{n} \llbracket\ d_i;Q_i\ \rrbracket, \{1\} \cap \sum_{i=1}^{n} Q_i)$

$\langle 7\rangle 1.$ $\{1\} \cap \sum_{i=1}^{n} Q'_i \subseteq \{1\} \cap \sum_{i=1}^{n} Q_i$

PROOF: By the overall assumption $(\forall i \leq n : Q'_i \subseteq Q_i)$

$\langle 7\rangle 2.$ $\oplus \bigcup_{i=1}^{n} \llbracket\ d_i;Q_i\ \rrbracket \rightsquigarrow_{nr} \oplus \bigcup_{i=1}^{n} \llbracket\ d'_i;Q'_i\ \rrbracket$

PROOF: By $\langle 2\rangle 1$ and Lemma 20

$\langle 7\rangle 3.$ $(\oplus \bigcup_{i=1}^{n} \llbracket\ d'_i;Q'_i\ \rrbracket, \{1\} \cap \sum_{i=1}^{n} Q'_i) \in \llbracket\ d'\ \rrbracket$

PROOF: By definition 9

$\langle 7\rangle 4.$ Q.E.D.

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 7\rangle 3$; $(\oplus \bigcup_{i=1}^{n} \llbracket\ d'_i;Q'_i\ \rrbracket, \{1\} \cap \sum_{i=1}^{n} Q'_i)$ is the $po'$ we are looking for

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

PROOF: By definition 9 the cases $\langle 6\rangle 1$ and $\langle 6\rangle 2$ are exhaustive

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

PROOF: $\Rightarrow$-rule

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

PROOF: $\forall$-rule

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

PROOF: By $\langle 3\rangle 1$

$\langle 2\rangle 3.$ $\forall po' \in \llbracket\ d'\ \rrbracket : \exists S \subseteq \llbracket\ d'\ \rrbracket, po \in \llbracket\ d\ \rrbracket : po' \in S \wedge po \rightsquigarrow_{pnr} \bar{\oplus} S$

$\langle 3\rangle 1.$ ASSUME: $po'_a \in \llbracket\ d'\ \rrbracket$
PROVE: $\exists S \subseteq \llbracket\ d'\ \rrbracket, po \in \llbracket\ d\ \rrbracket : po'_a \in S \wedge po \rightsquigarrow_{pnr} \bar{\oplus} S$

$\langle 4\rangle 1.$ LET: $po_a \in \llbracket\ d\ \rrbracket$ such that $po_a \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d\ \rrbracket$

PROOF: By Lemma 12

$\langle 4\rangle 2.$ $po_a \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\ d'\ \rrbracket$

$\langle 5\rangle 1.$ $\pi_1.po_a \rightsquigarrow_{nr} \oplus\llbracket\ d'\ \rrbracket$

$\langle 6\rangle 1.$ $\oplus\llbracket\ d\ \rrbracket = \oplus \bigcup_{i=1}^{n} \llbracket\ d_i\ \rrbracket \wedge \oplus\llbracket\ d'\ \rrbracket = \oplus \bigcup_{i=1}^{n} \llbracket\ d'_i\ \rrbracket$

PROOF: By definition 9 and definition 4

$\langle 6\rangle 2.$ $\oplus\llbracket\ d\ \rrbracket \rightsquigarrow_{nr} \oplus\llbracket\ d'\ \rrbracket$

PROOF: By $\langle 2\rangle 1$, $\langle 6\rangle 1$ and Lemma 20

$\langle 6\rangle 3.$ $\pi_1.po_a \rightsquigarrow_{nr} \oplus\llbracket\ d\ \rrbracket$

PROOF: By $\langle 4\rangle 1$

$\langle 6\rangle 4.$ Q.E.D.

PROOF: By $\langle 6\rangle 3$, $\langle 6\rangle 2$ and Theorem 5

$\langle 5\rangle 2.$ $\pi_2.\bar{\oplus}[\![\, d' \,]\!] \subseteq \pi_2.po_a$

$\langle 6\rangle 1.$ $\pi_2.\bar{\oplus}[\![\, d' \,]\!] \subseteq \pi_2.\bar{\oplus}[\![\, d \,]\!]$

PROOF: By the overall assumption and Lemma 21

$\langle 6\rangle 2.$ $\pi_2.\bar{\oplus}[\![\, d \,]\!] \subseteq \pi_2.po_a$

PROOF: By $\langle 4\rangle 1$

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

PROOF: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$

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

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

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

PROOF: By $\langle 4\rangle 1$ and $\langle 4\rangle 2$; $po_a$ is the $po$ we are looking for and $[\![\, d' \,]\!]$ is the $S$ we are looking for

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

PROOF: $\forall$-rule

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

PROOF: By $\langle 2\rangle 2$ and $\langle 2\rangle 3$

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

PROOF: $\Rightarrow$-rule

□

### Correspondence between $[\![\, d \,]\!]^i$ and $[\![\, g(d) \,]\!]^p$ w.r.t. compliance

**Theorem 1.** *Let* $d \in \mathcal{D}^i$. *Then*

$$(\forall (o,\{q\}) \in \langle I\rangle_d^p : q > 0) \wedge [\![\, d \,]\!]^i \mapsto_l \langle I\rangle_d^i \Rightarrow [\![\, g(d) \,]\!]^p \mapsto_{pl} \langle I\rangle_d^p$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: $\forall (o,\{q\}) \in \langle I\rangle_d^p : q > 0 \wedge [\![\, d \,]\!]^i \mapsto_l \langle I\rangle_d^i$

PROVE: $[\![\, g(d) \,]\!]^p \mapsto_{pl} \langle I\rangle_d^p$

$\langle 2\rangle 1.$ $\forall po \in [\![\, g(d) \,]\!]^p : 0 \notin Q \Rightarrow \exists po' \in \langle I\rangle_d^p : po \mapsto_{pr} po'$, i.e. $[\![\, g(d) \,]\!]^p \mapsto_{pg} \langle I\rangle_d^p$

$\langle 3\rangle 1.$ ASSUME: $po_1 \in [\![\, g(d) \,]\!]^p$

PROVE: $0 \notin Q_1 \Rightarrow \exists po' \in \langle I\rangle_d^p : po_1 \mapsto_{pr} po'$

$\langle 4\rangle 1.$ ASSUME: $0 \notin Q_1$

PROVE: $\exists po' \in \langle I\rangle_d^p : po_1 \mapsto_{pr} po'$

$\langle 5\rangle 1.$ CASE: $Q_1 = \{1\}$

$\langle 6\rangle 1.$ LET: $po_1' = ((traces(I), \mathcal{H}^{ll(d)} \setminus traces(I)), \{1\})$

$\langle 6\rangle 2.$ $po_1' \in \langle I\rangle_d^p$

PROOF: By definition 30

$\langle 6\rangle 3.$ $po_1 \mapsto_{pr} po_1'$

$\langle 7\rangle 1.$ $\{1\} \subseteq Q_1$

PROOF: By assumption $\langle 5\rangle 1$

$\langle 7\rangle 2.$ $o_1 \mapsto_r o_1'$

$\langle 8\rangle 1.$ $p_1 \subseteq p'_1 \cup n'_1$

$\langle 9\rangle 1.$ $p_1 \subseteq \mathcal{H}^{ll(d)}$

Proof: By assumption $\langle 3\rangle 1$

$\langle 9\rangle 2.$ $\mathcal{H}^{ll(d)} \subseteq traces(I) \cup \mathcal{H}^{ll(d)} \setminus traces(I)$

Proof: By set theory

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

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

$\langle 8\rangle 2.$ $n_1 \subseteq n'_1$, i.e. $n_1 \subseteq \mathcal{H}^{ll(d)} \setminus traces(I)$

$\langle 9\rangle 1.$ Assume: $t_1 \in n_1$
Prove: $t_1 \in n'_1$, i.e. $t_1 \in \mathcal{H}^{ll(d)} \setminus traces(I)$

$\langle 10\rangle 1.$ $t_1 \in \mathcal{H}^{ll(d)}$

Proof: By assumption $\langle 9\rangle 1$

$\langle 10\rangle 2.$ $t_1 \notin traces(I)$

$\langle 11\rangle 1.$ Assume: $t_1 \in traces(I)$
Prove: $\perp$

$\langle 12\rangle 1.$ $(\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\}) \in \langle I\rangle^i_d$

Proof: By assumption $\langle 11\rangle 1$

$\langle 12\rangle 2.$ Let: $o_2 \in [\![\ d\ ]\!]^i$ such that $o_2 \mapsto_r (\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\})$

Proof: By $\langle 12\rangle 1$ and assumption $\langle 1\rangle 1$ ($[\![\ d\ ]\!]^i \mapsto_l \langle I\rangle^i_d$)

$\langle 12\rangle 3.$ $t_1 \notin n_2$

Proof: By $\langle 12\rangle 2$

$\langle 12\rangle 4.$ $o_1 \rightsquigarrow_r o_2$

$\langle 13\rangle 1.$ $\forall po \in [\![\ g(d)\ ]\!]^p : o_1 \rightsquigarrow_r o$

Proof: By assumption $\langle 3\rangle 1$, assumption $\langle 5\rangle 1$ and Lemma 33

$\langle 13\rangle 2.$ $\forall o \in [\![\ d\ ]\!]^i : o_1 \rightsquigarrow_r o$

Proof: By $\langle 13\rangle 1$ and Lemma 34

$\langle 13\rangle 3.$ Q.E.D.

Proof: By $\langle 12\rangle 2$ ($o_2 \in [\![\ d\ ]\!]^i$) and $\langle 13\rangle 2$

$\langle 12\rangle 5.$ Q.E.D.

Proof: By $\langle 9\rangle 1$, $\langle 12\rangle 3$ and $\langle 12\rangle 4$

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

Proof: $\perp$-rule

$\langle 10\rangle 3.$ Q.E.D.

Proof: By $\langle 10\rangle 1$ and $\langle 10\rangle 2$

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

Proof: $\subseteq$-rule

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

Proof: By $\langle 8\rangle 1$ and $\langle 8\rangle 2$

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

Proof: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 6\rangle 1$

$\langle 6\rangle 4.$ Q.E.D.

Proof: By $\langle 6\rangle 2$ and $\langle 6\rangle 3$; $po'_1$ is the $po'$ we are looking for

$\langle 5\rangle 2.$ Case: $\langle 0,1] \subseteq Q_1$

$\langle 6\rangle 1.$ Let: $o_1' \in [\![\ d\ ]\!]^i$ s.t. $o_1 \rightsquigarrow_r o_1'$

Proof: By assumption $\langle 3\rangle 1$ and Lemma 35

$\langle 6\rangle 2.$ Let: $t_1 \in \mathit{traces}(I)$ s.t. $o_1' \mapsto_r (\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\})$

Proof: By $\langle 6\rangle 1$ ($o_1' \in [\![\ d\ ]\!]^i$) and assumption $\langle 1\rangle 1$ ($[\![\ d\ ]\!]^i \mapsto_l \langle I\rangle_d^i$)

$\langle 6\rangle 3.$ $o_1 \mapsto_r (\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\})$

Proof: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and transitivity of $\rightsquigarrow_r$ and $\mapsto_r$ (which are identical)

$\langle 6\rangle 4.$ Let: $q_1 \in [0,1]$ s.t. $((\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\}), \{q_1\}) \in \langle I\rangle_d^p$

Proof: By $\langle 6\rangle 2$ and Lemma 28

$\langle 6\rangle 5.$ $q_1 > 0$

Proof: By $\langle 6\rangle 4$ and assumption $\langle 1\rangle 1$ ($\forall (o, \{q\}) \in \langle I\rangle_d^p : q > 0$)

$\langle 6\rangle 6.$ $\{q_1\} \subseteq Q_1$

Proof: By assumption $\langle 5\rangle 2$ and $\langle 6\rangle 5$

$\langle 6\rangle 7.$ Q.E.D.

Proof: By $\langle 6\rangle 3$, $\langle 6\rangle 4$ and $\langle 6\rangle 6$; $((\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\}), \{q_1\})$ is the $po'$ we are looking for

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

Proof: By Lemma 32 the cases $\langle 5\rangle 1$ and $\langle 5\rangle 2$ are exhaustive

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

Proof: $\Rightarrow$-rule

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

Proof: $\forall$-rule

$\langle 2\rangle 2.$ $\forall po' \in \langle I\rangle_d^p : \exists S \subseteq \langle I\rangle_d^p : \exists po \in [\![\ g(d)\ ]\!]^p : po' \in S \wedge po \mapsto_{pr} \bar{\oplus} S$

$\langle 3\rangle 1.$ Assume: $po_1' \in \langle I\rangle_d^p$

Prove: $\exists S \subseteq \langle I\rangle_d^p : \exists po \in [\![\ g(d)\ ]\!]^p : po_1' \in S \wedge po \mapsto_{pr} \bar{\oplus} S$

$\langle 4\rangle 1.$ Let: $po_2' = \bar{\oplus} \langle I\rangle_d^p$

$\langle 4\rangle 2.$ Let: $po_2 \in [\![\ g(d)\ ]\!]$ s.t. $Q_2 = \{1\}$

Proof: By Lemma 36

$\langle 4\rangle 3.$ $po_2 \mapsto_{pr} po_2'$

$\langle 5\rangle 1.$ $Q_2' \subseteq Q_2$

$\langle 6\rangle 1.$ $Q_2' = \{1\}$

$\langle 7\rangle 1.$ $\forall po \in \langle I\rangle_d^p : \exists q \in Q : q \in [0,1]$

Proof: By definition 30

$\langle 7\rangle 2.$ $\exists po \in \langle I\rangle_d^p : Q = \{1\}$

Proof: By definition 30

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

Proof: By $\langle 4\rangle 1$, $\langle 7\rangle 1$, $\langle 7\rangle 2$ and definition 7

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

Proof: By $\langle 4\rangle 2$ and $\langle 6\rangle 1$

$\langle 5\rangle 2.$ $o_2 \mapsto_r o_2'$

$\langle 6\rangle 1.$ $p_2 \subseteq p_2' \cup n_2'$

$\langle 7\rangle 1.$ $p_2 \subseteq \mathcal{H}^{ll(d)}$

Proof: By $\langle 4\rangle 2$

$\langle 7\rangle 2.$ $\mathcal{H}^{ll(d)} \subseteq p_2' \cup n_2'$

$\langle 8\rangle 1.$ $\forall po \in \langle I\rangle_d^p : \mathcal{H}^{ll(d)} \subseteq p \cup n$

PROOF: By definition 30

$\langle 8\rangle 2.$ Q.E.D.

PROOF: By $\langle 8\rangle 1$ and definition 4

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

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

$\langle 6\rangle 2.$ $n_2 \subseteq n_2'$

$\langle 7\rangle 1.$ ASSUME: $t_2 \in n_2$

PROVE: $t_2 \in n_2'$

$\langle 8\rangle 1.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : o_2 \rightsquigarrow_r o$

PROOF: By $\langle 4\rangle 2$ and Lemma 33

$\langle 8\rangle 2.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : t_2 \in n$

PROOF: By $\langle 8\rangle 1$ and assumption $\langle 7\rangle 1$

$\langle 8\rangle 3.$ $t_2 \notin traces(I)$

$\langle 9\rangle 1.$ ASSUME: $t_2 \in traces(I)$

PROVE: $\perp$

$\langle 10\rangle 1.$ $(\{t_2\}, \mathcal{H}^{ll(d)} \setminus \{t_2\}) \in \langle I\rangle_d^i$

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

$\langle 10\rangle 2.$ LET: $o_3 \in \llbracket\ d\ \rrbracket^i$ s.t. $o_3 \mapsto_r (\{t_2\}, \mathcal{H}^{ll(d)} \setminus \{t_2\})$

PROOF: By $\langle 10\rangle 1$ and assumption $\langle 1\rangle 1$ ($\llbracket\ d\ \rrbracket^i \mapsto_l \langle I\rangle_d^i$)

$\langle 10\rangle 3.$ $t_2 \notin n_3$

PROOF: By $\langle 10\rangle 2$

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

PROOF: By $\langle 8\rangle 2$, $\langle 10\rangle 2$ and $\langle 10\rangle 3$

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

PROOF: $\perp$-rule

$\langle 8\rangle 4.$ $t_2 \in \mathcal{H}^{ll(d)}$

PROOF: By assumption $\langle 7\rangle 1$

$\langle 8\rangle 5.$ $\forall po \in \langle I\rangle_d^p : t_2 \in n$

PROOF: By $\langle 8\rangle 4$ and $\langle 8\rangle 3$

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

PROOF: By $\langle 8\rangle 5$

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

PROOF: $\subseteq$-rule

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

PROOF: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$

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

PROOF: By $\langle 5\rangle 1$ and $\langle 5\rangle 2$

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

PROOF: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and $\langle 4\rangle 3$;$\langle I\rangle_d^p$ is the $S$ we are looking for and $po_2$ is the $po$ we are looking for

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

PROOF: $\forall$-rule

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

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

⟨1⟩2. Q.E.D.
PROOF: ⇒-rule

□

Lemma 55 shows why the conjunct $\forall(o, \{q\}) \in \langle I \rangle_d^p : q > 0$ is included in the antecedent of Theorem 1.

**Lemma 55 (Non-correspondence between $\mapsto_l$ and $\mapsto_{pl}$).** *Let $d \in \mathcal{D}^i$. Then*

$$[\![\ d\ ]\!]^i \mapsto_l \langle I \rangle_d^i \not\Rightarrow [\![\ g(d)\ ]\!]^p \mapsto_{pl} \langle I \rangle_d^p$$

PROOF. Let

$$d = \mathsf{refuse}(a \ \mathsf{xalt}\ ab)$$

and let $I$ be the program

```
output a;
while random(0.5) skip;
output b;
```

where `random(0.5)` returns either *true* (with a probability of 0.5) or *false*, and `skip` is a programming construct for doing nothing. The program $I$ will produce the trace $\langle a \rangle$ only if `random(0.5)` returns true infinitely many times, otherwise it produces $\langle ab \rangle$. In the non-probabilistic case we get

$$\begin{aligned} [\![\ d\ ]\!]^i &= \{\ (\emptyset, \{\langle a \rangle\}), (\emptyset, \{\langle ab \rangle\})\ \} \\ traces(I) &= \{\langle a \rangle, \langle ab \rangle\} \\ \langle I \rangle_d^i &= \{\ (\{\langle a \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle\}), (\{\langle ab \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle ab \rangle\})\ \} \end{aligned}$$

This means that $[\![\ d\ ]\!]^i \mapsto_l \langle I \rangle_d^i$, since $(\emptyset, \{\langle a \rangle\}) \mapsto_r (\{\langle ab \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle ab \rangle\})$ and $(\emptyset, \{\langle ab \rangle\}) \mapsto_r (\{\langle a \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle\})$.

The probability of producing the trace $\langle a \rangle$ is $0.5^\infty = 0$. In the probabilistic case we get

$$\begin{aligned} [\![\ g(d)\ ]\!]^p &= \{\ ((\emptyset, \{\langle a \rangle\}), \langle 0, 1]), ((\emptyset, \{\langle ab \rangle\}), \langle 0, 1]), ((\emptyset, \emptyset), \langle 0, 1]), ((\emptyset, \emptyset), \{1\})\ \} \\ \langle I \rangle_d^p &= \{\ ((\{\langle a \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle\}), \{0\}), ((\{\langle ab \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle ab \rangle\}), \{1\}), \\ &\quad ((\{\langle a \rangle, \langle ab \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle, \langle ab \rangle\}), \{1\})\ \} \end{aligned}$$

So $[\![\ d\ ]\!]^p \mapsto_{pl} \langle I \rangle_d^p$ does not hold, because the p-obligation $((\emptyset, \{\langle ab \rangle\}), \langle 0, 1])$ is not represented by any p-obligation in $\langle I \rangle_d^p$. □

**Theorem 2.** *Let $d \in \mathcal{D}^i$. Then*

$$E(d) \wedge (\forall(o, \{q\}) \in \langle I \rangle_d^p : q > 0) \wedge [\![\ d\ ]\!]^i \mapsto_{nl} \langle I \rangle_d^i \Rightarrow [\![\ g(d)\ ]\!]^p \mapsto_{pnl} \langle I \rangle_d^p$$

PROOF.

⟨1⟩1. ASSUME: 1. $E(d)$
2. $\forall(o, \{q\}) \in \langle I \rangle_d^p : q > 0$

3. $\llbracket\ d\ \rrbracket^i \mapsto_{nl} \langle I\rangle^i_d$

PROVE: $\llbracket\ g(d)\ \rrbracket^p \mapsto_{pnl} \langle I\rangle^p_d$

$\langle 2\rangle$1. $\forall po \in \llbracket\ g(d)\ \rrbracket^p : 0 \notin Q \Rightarrow \exists po' \in \langle I\rangle^p_d : po \mapsto_{pnr} po'$, i.e. $\llbracket\ g(d)\ \rrbracket^p \mapsto_{pg} \langle I\rangle^p_d$

$\langle 3\rangle$1. ASSUME: $po_1 \in \llbracket\ g(d)\ \rrbracket^p$

PROVE: $0 \notin Q_1 \Rightarrow \exists po' \in \langle I\rangle^p_d : po_1 \mapsto_{pnr} po'$

$\langle 4\rangle$1. ASSUME: $0 \notin Q_1$

PROVE: $\exists po' \in \langle I\rangle^p_d : po_1 \mapsto_{pnr} po'$

$\langle 5\rangle$1. CASE: $Q_1 = \{1\}$

$\langle 6\rangle$1. LET: $po'_1 = ((traces(I), \mathcal{H}^{ll(d)} \setminus traces(I)), \{1\})$

$\langle 6\rangle$2. $po'_1 \in \langle I\rangle^p_d$

PROOF: By definition 30

$\langle 6\rangle$3. $po_1 \mapsto_{pnr} po'_1$

$\langle 7\rangle$1. $\{1\} \subseteq Q_1$

PROOF: By assumption $\langle 5\rangle$1

$\langle 7\rangle$2. $o_1 \mapsto_{nr} o'_1$

$\langle 8\rangle$1. $p_1 \subseteq p'_1 \cup n'_1$

$\langle 9\rangle$1. $p_1 \subseteq \mathcal{H}^{ll(d)}$

PROOF: By assumption $\langle 3\rangle$1

$\langle 9\rangle$2. $\mathcal{H}^{ll(d)} \subseteq traces(I) \cup \mathcal{H}^{ll(d)} \setminus traces(I)$

PROOF: By set theory

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

PROOF: By $\langle 9\rangle$1 and $\langle 9\rangle$2

$\langle 8\rangle$2. $n_1 \subseteq n'_1$, i.e. $n_1 \subseteq \mathcal{H}^{ll(d)} \setminus traces(I)$

$\langle 9\rangle$1. ASSUME: $t_1 \in n_1$

PROVE: $t_1 \in n'_1$, i.e. $t_1 \in \mathcal{H}^{ll(d)} \setminus traces(I)$

$\langle 10\rangle$1. $t_1 \in \mathcal{H}^{ll(d)}$

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

$\langle 10\rangle$2. $t_1 \notin traces(I)$

$\langle 11\rangle$1. ASSUME: $t_1 \in traces(I)$

PROVE: $\bot$

$\langle 12\rangle$1. $(\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\}) \in \langle I\rangle^i_d$

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

$\langle 12\rangle$2. LET: $o_2 \in \llbracket\ d\ \rrbracket^i$ such that
$o_2 \mapsto_{nr} (\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\})$

PROOF: By $\langle 12\rangle$1 and assumption $\langle 1\rangle$1.3

$\langle 12\rangle$3. $t_1 \notin n_2$

PROOF: By $\langle 12\rangle$2

$\langle 12\rangle$4. $o_1 \rightsquigarrow_r o_2$

$\langle 13\rangle$1. $\forall po \in \llbracket\ g(d)\ \rrbracket^p : o_1 \rightsquigarrow_r o$

PROOF: By assumption $\langle 3\rangle$1, assumption $\langle 5\rangle$1 and Lemma 33

$\langle 13\rangle$2. $\forall o \in \llbracket\ d\ \rrbracket^i : o_1 \rightsquigarrow_r o$

PROOF: By $\langle 13\rangle$1 and Lemma 34

$\langle 13\rangle$3. Q.E.D.

PROOF: By $\langle 12\rangle 2$ ($o_2 \in [\![ \ d \ ]\!]^i$) and $\langle 13\rangle 2$

$\langle 12\rangle 5.$ $t_1 \notin n_1$

PROOF: By $\langle 12\rangle 3$ and $\langle 12\rangle 4$

$\langle 12\rangle 6.$ Q.E.D.

PROOF: By $\langle 12\rangle 5$ and $\langle 9\rangle 1$

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

PROOF: $\perp$-rule

$\langle 10\rangle 3.$ Q.E.D.

PROOF: By $\langle 10\rangle 1$ and $\langle 10\rangle 2$

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

PROOF: $\subseteq$-rule

$\langle 8\rangle 3.$ $p_1 \cap p_1' \neq \emptyset$

$\langle 9\rangle 1.$ LET: $o_3 \in [\![ \ d \ ]\!]^i$ s.t. $o_1 \rightsquigarrow_{nr} o_3$

PROOF: By assumption $\langle 1\rangle 1.1$, assumption $\langle 3\rangle 1$ and Lemma 44

$\langle 9\rangle 2.$ LET: $t \in traces(I)$ s.t. $(\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\}) \in \langle I\rangle_d^i \wedge$
$(p_3, n_3) \mapsto_{nr} (\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\})$

PROOF: By assumption $\langle 1\rangle 1.3$

$\langle 9\rangle 3.$ $t \in p_3$

PROOF: By $\langle 9\rangle 2$

$\langle 9\rangle 4.$ $t \in p_1$

PROOF: By $\langle 9\rangle 3$ and $\langle 9\rangle 1$

$\langle 9\rangle 5.$ $t \in p_1'$

PROOF: By $\langle 6\rangle 1$ and $\langle 9\rangle 2$ ($t \in traces(I)$)

$\langle 9\rangle 6.$ Q.E.D.

PROOF: By $\langle 9\rangle 4$ and $\langle 9\rangle 5$

$\langle 8\rangle 4.$ Q.E.D.

PROOF: By $\langle 8\rangle 1$, $\langle 8\rangle 2$ and $\langle 8\rangle 3$

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

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 6\rangle 1$

$\langle 6\rangle 4.$ Q.E.D.

PROOF: By $\langle 6\rangle 2$ and $\langle 6\rangle 3$; $po_1'$ is the $po'$ we are looking for

$\langle 5\rangle 2.$ CASE: $\langle 0, 1] \subseteq Q_1$

$\langle 6\rangle 1.$ LET: $o_1' \in [\![ \ d \ ]\!]^i$ s.t. $o_1 \rightsquigarrow_{nr} o_1'$

PROOF: By assumption $\langle 3\rangle 1$, assumption $\langle 1\rangle 1.1$ and Lemma 44

$\langle 6\rangle 2.$ LET: $t_1 \in traces(I)$ s.t. $o_1' \mapsto_{nr} (\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\})$

PROOF: By $\langle 6\rangle 1$ ($o_1' \in [\![ \ d \ ]\!]^i$) and assumption $\langle 1\rangle 1.3$

$\langle 6\rangle 3.$ $o_1 \mapsto_{nr} (\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\})$

PROOF: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and Theorem 6

$\langle 6\rangle 4.$ LET: $q_1 \in [0, 1]$ s.t. $((\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\}), \{q_1\}) \in \langle I\rangle_d^p$

PROOF: By $\langle 6\rangle 2$ and Lemma 28

$\langle 6\rangle 5.$ $q_1 > 0$

PROOF: By $\langle 6\rangle 4$ and assumption $\langle 1\rangle 1.2$

$\langle 6\rangle 6.$ $\{q_1\} \subseteq Q_1$

PROOF: By assumption $\langle 5\rangle 2$ and $\langle 6\rangle 5$

⟨6⟩7. Q.E.D.

PROOF: By ⟨6⟩3, ⟨6⟩4 and ⟨6⟩6; $((\{t_1\}, \mathcal{H}^{ll(d)} \setminus \{t_1\}), \{q_1\})$ is the $po'$ we are looking for

⟨5⟩3. Q.E.D.

PROOF: By Lemma 32 the cases ⟨5⟩1 and ⟨5⟩2 are exhaustive

⟨4⟩2. Q.E.D.

PROOF: $\Rightarrow$-rule

⟨3⟩2. Q.E.D.

PROOF: $\forall$-rule

⟨2⟩2. $\forall po' \in \langle I \rangle_d^p : \exists S \subseteq \langle I \rangle_d^p : \exists po \in [\![\ g(d)\ ]\!]^p : po' \in S \wedge po \mapsto_{pnr} \bar{\oplus} S$

⟨3⟩1. ASSUME: $po'_1 \in \langle I \rangle_d^p$
PROVE: $\exists S \subseteq \langle I \rangle_d^p : \exists po \in [\![\ g(d)\ ]\!]^p : po' \in S \wedge po \mapsto_{pnr} \bar{\oplus} S$

⟨4⟩1. LET: $po'_2 = \bar{\oplus} \langle I \rangle_d^p$

⟨4⟩2. LET: $po_2 \in [\![\ g(d)\ ]\!]$ s.t. $Q_2 = \{1\}$

PROOF: By Lemma 36

⟨4⟩3. $po_2 \mapsto_{pnr} po'_2$

⟨5⟩1. $Q'_2 \subseteq Q_2$

⟨6⟩1. $Q'_2 = \{1\}$

⟨7⟩1. $\forall po \in \langle I \rangle_d^p : \exists q \in Q : q \in [0, 1]$

PROOF: By definition 30

⟨7⟩2. $\exists po \in \langle I \rangle_d^p : Q = \{1\}$

PROOF: By definition 30

⟨7⟩3. Q.E.D.

PROOF: By ⟨4⟩1, ⟨7⟩1, ⟨7⟩2 and definition 7

⟨6⟩2. Q.E.D.

PROOF: By ⟨4⟩2 and ⟨6⟩1

⟨5⟩2. $o_2 \mapsto_r o'_2$

⟨6⟩1. $p_2 \subseteq p'_2 \cup n'_2$

⟨7⟩1. $p_2 \subseteq \mathcal{H}^{ll(d)}$

PROOF: By ⟨4⟩2

⟨7⟩2. $\mathcal{H}^{ll(d)} \subseteq p'_2 \cup n'_2$

⟨8⟩1. $\forall po \in \langle I \rangle_d^p : \mathcal{H}^{ll(d)} \subseteq p \cup n$

PROOF: By definition 30

⟨8⟩2. Q.E.D.

PROOF: By ⟨8⟩1 and definition 4

⟨7⟩3. Q.E.D.

PROOF: By ⟨7⟩1 and ⟨7⟩2

⟨6⟩2. $n_2 \subseteq n'_2$

⟨7⟩1. ASSUME: $t_2 \in n_2$
PROVE: $t_2 \in n'_2$

⟨8⟩1. $\forall po \in [\![\ g(d)\ ]\!]^p : o_2 \rightsquigarrow_r o$

PROOF: By ⟨4⟩2 and Lemma 33

⟨8⟩2. $\forall po \in [\![\ g(d)\ ]\!]^p : t_2 \in n$

PROOF: By ⟨8⟩1 and assumption ⟨7⟩1

⟨8⟩3. $t_2 \notin traces(I)$

$\langle 9\rangle 1.$ Assume: $t_2 \in \mathit{traces}(I)$
Prove: $\bot$

$\langle 10\rangle 1.$ $(\{t_2\}, \mathcal{H}^{ll(d)} \setminus \{t_2\}) \in \langle I\rangle_d^i$
Proof: By assumption $\langle 9\rangle 1$

$\langle 10\rangle 2.$ Let: $o_3 \in [\![\ d\ ]\!]^i$ s.t. $o_3 \mapsto_{nr} (\{t_2\}, \mathcal{H}^{ll(d)} \setminus \{t_2\})$
Proof: By $\langle 10\rangle 1$ and assumption $\langle 1\rangle 1.3$

$\langle 10\rangle 3.$ $t_2 \notin n_3$
Proof: By $\langle 10\rangle 2$

$\langle 10\rangle 4.$ $\forall o \in [\![\ d\ ]\!]^i : t_2 \in n$
Proof: By $\langle 8\rangle 2$ and Lemma 34

$\langle 10\rangle 5.$ Q.E.D.
Proof: By $\langle 10\rangle 2$, $\langle 10\rangle 3$ and $\langle 10\rangle 4$

$\langle 9\rangle 2.$ Q.E.D.
Proof: $\bot$-rule

$\langle 8\rangle 4.$ $t_2 \in \mathcal{H}^{ll(d)}$
Proof: By assumption $\langle 7\rangle 1$

$\langle 8\rangle 5.$ $\forall po \in \langle I\rangle_d^p : t_2 \in n$
Proof: By $\langle 8\rangle 4$ and $\langle 8\rangle 3$

$\langle 8\rangle 6.$ Q.E.D.
Proof: By $\langle 8\rangle 5$

$\langle 7\rangle 2.$ Q.E.D.
Proof: $\subseteq$-rule

$\langle 6\rangle 3.$ Q.E.D.
Proof: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$

$\langle 5\rangle 3.$ $p_2 \cap p_2' \neq \emptyset$

$\langle 6\rangle 1.$ Let: $o_3 \in [\![\ d\ ]\!]^i$ s.t. $o_2 \rightsquigarrow_{nr} o_3$
Proof: By assumption $\langle 1\rangle 1.1$ and Lemma 44

$\langle 6\rangle 2.$ Let: $t \in \mathit{traces}(I)$ s.t. $(\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\}) \in \langle I\rangle_d^i \wedge$
$o_3 \mapsto_{nr} (\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\})$
Proof: By assumption $\langle 1\rangle 1.3$

$\langle 6\rangle 3.$ $o_2 \mapsto_{nr} (\{t\}, \mathcal{H}^{ll(d)} \setminus \{t\})$
Proof: By $\langle 6\rangle 1$, $\langle 6\rangle 2$ and Theorem 6

$\langle 6\rangle 4.$ $t \in p_2$
Proof: By $\langle 6\rangle 3$

$\langle 6\rangle 5.$ $p_2' = \mathit{traces}(I)$
Proof: By $\langle 4\rangle 1$

$\langle 6\rangle 6.$ Q.E.D.
Proof: By $\langle 6\rangle 4$, $\langle 6\rangle 5$ and $\langle 6\rangle 2$ ($t \in \mathit{traces}(I)$)

$\langle 5\rangle 4.$ Q.E.D.
Proof: By $\langle 5\rangle 1$, $\langle 5\rangle 2$ and $\langle 5\rangle 3$

$\langle 4\rangle 4.$ Q.E.D.
Proof: By $\langle 4\rangle 1$, $\langle 4\rangle 2$ and $\langle 4\rangle 3$;$\langle I\rangle_d^p$ is the $S$ we are looking for and $po_2$ is the $po$ we are looking for

$\langle 3\rangle 2.$ Q.E.D.
Proof: $\forall$-rule

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

Proof: By $\langle 2 \rangle 1$ and $\langle 2 \rangle 2$

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

Proof: $\Rightarrow$-rule

□

Lemma 56 and Lemma 57 show why stronger formulations of Theorem 2 does not hold.

**Lemma 56 (Non-correspondence between $\mapsto_{nl}$ and $\mapsto_{pnl}$).** *Let $d \in \mathcal{D}^i$. Then*

$$(\forall (o, \{q\}) \in \langle I \rangle^p_d : q > 0 \wedge \llbracket\ d\ \rrbracket^i \mapsto_{nl} \langle I \rangle^i_d) \not\Rightarrow \llbracket\ g(d)\ \rrbracket^p \mapsto_{pnl} \langle I \rangle^p_d$$

Proof. Let $d = a$ $\mathsf{xalt}$ $b$ and $\mathit{traces}(I) = \{\langle a \rangle, \langle b \rangle\}$. This gives

$$\begin{aligned}
\llbracket\ d\ \rrbracket^i &= \{\ (\{\langle a \rangle\}, \emptyset), (\{\langle b \rangle\}, \emptyset)\ \} \\
\langle I \rangle^i_d &= \{\ (\{\langle a \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle\}), (\{\langle b \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle b \rangle\})\ \} \\
\llbracket\ g(d)\ \rrbracket^p &= \{\ ((\{\langle a \rangle\}, \emptyset), \langle 0, 1]), ((\{\langle b \rangle\}, \emptyset), \langle 0, 1]), ((\emptyset, \emptyset), \langle 0, 1]), ((\emptyset, \emptyset), \{1\})\ \} \\
\langle I \rangle^p_d &= \{\ ((\{\langle a \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle\}), \{q_1\}), ((\{\langle b \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle b \rangle\}), \{q_2\}), \\
&\qquad ((\{\langle a \rangle, \langle b \rangle\}, \mathcal{H}^{ll(d)} \setminus \{\langle a \rangle, \langle b \rangle\}), \{1\})\ \}
\end{aligned}$$

for some $q_1, q_2 > 0$ such that $q_1 + q_2 = 1$. This means that

$$\llbracket\ d\ \rrbracket^i \mapsto_{nl} \langle I \rangle^i_d$$

since each interaction obligation in $\llbracket\ d\ \rrbracket^i$ is refined by an obligation in $\langle I \rangle^i_d$ with the same positive trace, and vice versa. But we also have

$$\llbracket\ g(d)\ \rrbracket^p \not\mapsto_{pnl} \langle I \rangle^p_d,$$

since the no p-obligation in $\langle I \rangle^p_d$ complies with $((\emptyset, \emptyset), \{1\})$ when using $\mapsto_{nr}$. This is because the set of positive traces is empty. □

**Lemma 57 (Non-correspondence between $\mapsto_{nl}$ and $\mapsto_{pnl}$).** *Let $d \in \mathcal{D}^i$. Then*

$$\begin{aligned}
&(\exists s \in \mathbb{P}(\mathcal{H}) : \forall (p, n) \in \llbracket\ d\ \rrbracket^i : p \cup n = s \wedge \\
&\forall (o, \{q\}) \in \langle I \rangle^p_d : q > 0 \wedge \\
&\llbracket\ d\ \rrbracket^i \mapsto_{nl} \langle I \rangle^i_d) \\
&\not\Rightarrow \\
&\llbracket\ g(d)\ \rrbracket^p \mapsto_{pnl} \langle I \rangle^p_d
\end{aligned}$$

Proof. Let

$$\begin{aligned}
d_1 &= a\ \mathsf{xalt}\ aa \\
d_2 &= b\ \mathsf{alt}\ ab \\
d_3 &= ab\ \mathsf{alt}\ aaab \\
d &= (d_1\ \mathsf{seq}\ d_2)\ \mathsf{alt}\ d_3 \\
\mathit{traces}(I) &= \{\langle aab \rangle\}
\end{aligned}$$

For the non-probabilistic case this means that

$$\begin{aligned}
\llbracket\ d_1\ \rrbracket^i &= \{\ (\{\langle a\rangle\},\emptyset),(\{\langle aa\rangle\},\emptyset)\ \}\\
\llbracket\ d_1\ \mathsf{seq}\ d_2\ \rrbracket^i &= \{\ (\{\langle ab\rangle,\langle aab\rangle\},\emptyset),(\{\langle aab\rangle,\langle aaab\rangle\},\emptyset)\ \}\\
\llbracket\ d\ \rrbracket^i &= \{\ (\{\langle ab\rangle,\langle aab\rangle,\langle aaab\rangle\},\emptyset)\}\\
\langle I\rangle^i_d &= \{\ (\{\langle aab\rangle\},\mathcal{H}^{ll(d)}\setminus\{\langle aab\rangle\})\ \}
\end{aligned}$$

So $\llbracket\ d\ \rrbracket^i \mapsto_{nl} \langle I\rangle^i_d$ holds. In the probabilistic case we get

$$\begin{aligned}
\llbracket\ g(d_1)\ \rrbracket^p &= \{\ ((\{\langle a\rangle\},\emptyset),\langle 0,1]),((\{\langle aa\rangle\},\emptyset),\langle 0,1]),\\
&\qquad((\emptyset,\emptyset),\langle 0,1]),((\emptyset,\emptyset),\{1\})\ \}\\
\llbracket\ g(d_1\ \mathsf{seq}\ d_2)\ \rrbracket^p &= \{\ ((\{\langle ab\rangle,\langle aab\rangle\},\emptyset),\langle 0,1]),((\{\langle aab\rangle,\langle aaab\rangle\},\emptyset),\langle 0,1]),\\
&\qquad((\emptyset,\emptyset),\langle 0,1]),((\emptyset,\emptyset),\{1\})\ \}\\
\llbracket\ g(d)\ \rrbracket^p &= \{\ ((\{\langle ab\rangle,\langle aab\rangle,\langle aaab\rangle\},\emptyset),\langle 0,1]),\\
&\qquad((\{\langle ab\rangle,\langle aaab\rangle\},\emptyset),\langle 0,1]),((\{\langle ab\rangle,\langle aaab\rangle\},\emptyset),\{1\})\ \}\\
\langle I\rangle^p_d &= \{\ ((\{\langle aab\rangle\},\mathcal{H}^{ll(d)}\setminus\{\langle aab\rangle\}),\{1\})\ \}
\end{aligned}$$

We see that

$$\begin{aligned}
&\exists s\in\mathbb{P}(\mathcal{H}):\forall(p,n)\in\llbracket\ d\ \rrbracket^i:p\cup n=s\ \wedge\\
&\forall(o,\{q\})\in\langle I\rangle^p_d:q>0\ \wedge\\
&\llbracket\ d\ \rrbracket^i\mapsto_{nl}\langle I\rangle^i_d)
\end{aligned}$$

holds. But $\llbracket\ g(d)\ \rrbracket^p \mapsto_{pnl} \langle I\rangle^p_d$ does not hold, since $\{\langle ab\rangle,\langle aaab\rangle\}\cap\{\langle aab\rangle\}=\emptyset$, so not all p-obligations in $\llbracket\ d\ \rrbracket^p$ are represented in $\langle I\rangle^p_d$ when using $\mapsto_{pnr}$. □

### Correspondence between $\llbracket\ d\ \rrbracket^i$ and $\llbracket\ g(d)\ \rrbracket^p$ w.r.t. refinement

**Theorem 3.** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$N(d')\wedge E(d')\wedge\llbracket\ d\ \rrbracket^i\rightsquigarrow_l\llbracket\ d'\ \rrbracket^i\Rightarrow\llbracket\ g(d)\ \rrbracket^p\rightsquigarrow_{pl}\llbracket\ g(d')\ \rrbracket^p$$

PROOF.

$\langle 1\rangle 1.$ ASSUME: 1. $N(d')$
2. $E(d')$
3. $\llbracket\ d\ \rrbracket^i\rightsquigarrow_l\llbracket\ d'\ \rrbracket^i$
PROVE: $\llbracket\ g(d)\ \rrbracket^p\rightsquigarrow_{pl}\llbracket\ g(d')\ \rrbracket^p$

$\langle 2\rangle 1.$ LET: $s\in\mathbb{P}(\mathcal{H}):\forall(p,n)\in\llbracket\ d'\ \rrbracket^i:p\cup n=s$
PROOF: By assumption $\langle 1\rangle 1.1$ and assumption $\langle 1\rangle 1.2$

$\langle 2\rangle 2.$ $\forall po\in\llbracket\ g(d)\ \rrbracket^p:0\notin Q\Rightarrow\exists po'\in\llbracket\ g(d')\ \rrbracket^p:po\rightsquigarrow_{pr}po'$

$\langle 3\rangle 1.$ ASSUME: $po_1\in\llbracket\ g(d)\ \rrbracket^p$
PROVE: $0\notin Q_1\Rightarrow\exists po'\in\llbracket\ g(d')\ \rrbracket^p:po_1\rightsquigarrow_{pr}po'$

$\langle 4\rangle 1.$ ASSUME: $0\notin Q_1$
PROVE: $\exists po'\in\llbracket\ g(d')\ \rrbracket^p:po_1\rightsquigarrow_{pr}po'$

$\langle 5\rangle 1.$ Case: $Q_1 = \{1\}$
$\langle 6\rangle 1.$ Let: $po'_1 \in [\![ g(d') ]\!]^p$ s.t. $Q'_1 = \{1\}$
Proof: By Lemma 36
$\langle 6\rangle 2.$ $po_1 \rightsquigarrow_{pr} po'_1$
$\langle 7\rangle 1.$ $o_1 \rightsquigarrow_r o'_1$
$\langle 8\rangle 1.$ $\forall po \in [\![ g(d) ]\!]^p : o_1 \rightsquigarrow_r o$
Proof: By assumption $\langle 3\rangle 1$, assumption $\langle 5\rangle 1$ and Lemma 33
$\langle 8\rangle 2.$ $p_1 \subseteq p'_1 \cup n'_1$
$\langle 9\rangle 1.$ $\forall po \in [\![ g(d) ]\!]^p : p_1 \subseteq p \cup n$
Proof: By $\langle 8\rangle 1$
$\langle 9\rangle 2.$ $\forall o \in [\![ d ]\!]^i : p_1 \subseteq p \cup n$
Proof: By $\langle 9\rangle 1$ and Lemma 34
$\langle 9\rangle 3.$ $\forall o \in [\![ d' ]\!]^i : p_1 \subseteq p \cup n$
Proof: By $\langle 9\rangle 2$ and assumption $\langle 1\rangle 1.3$
$\langle 9\rangle 4.$ $\forall po \in [\![ g(d') ]\!]^p : p_1 \subseteq p \cup n$
Proof: By $\langle 9\rangle 3$, assumption $\langle 1\rangle 1.1$, $\langle 2\rangle 1$ and Lemma 39
$\langle 9\rangle 5.$ Q.E.D.
Proof: By $\langle 9\rangle 4$ and $\langle 6\rangle 1$ ($po'_1 \in [\![ g(d') ]\!]^p$)
$\langle 8\rangle 3.$ $n_1 \subseteq n'_1$
$\langle 9\rangle 1.$ $\forall po \in [\![ g(d) ]\!]^p : n_1 \subseteq n$
Proof: By $\langle 8\rangle 1$
$\langle 9\rangle 2.$ $\forall o \in [\![ d ]\!]^i : n_1 \subseteq n$
Proof: By $\langle 9\rangle 1$ and Lemma 34
$\langle 9\rangle 3.$ $\forall o \in [\![ d' ]\!]^i : n_1 \subseteq n$
Proof: By $\langle 9\rangle 2$ and assumption $\langle 1\rangle 1.3$
$\langle 9\rangle 4.$ $\forall po \in [\![ g(d') ]\!]^p : n_1 \subseteq n$
Proof: By $\langle 9\rangle 3$, assumption $\langle 1\rangle 1.1$, $\langle 2\rangle 1$ and Lemma 39
$\langle 9\rangle 5.$ Q.E.D.
Proof: By $\langle 9\rangle 4$ and $\langle 6\rangle 1$
$\langle 8\rangle 4.$ Q.E.D.
Proof: By $\langle 8\rangle 2$ and $\langle 8\rangle 3$
$\langle 7\rangle 2.$ $Q'_1 \subseteq Q_1$
Proof: By assumption $\langle 5\rangle 1$ and $\langle 6\rangle 1$
$\langle 7\rangle 3.$ Q.E.D.
Proof: By $\langle 7\rangle 1$ and $\langle 7\rangle 2$
$\langle 6\rangle 3.$ Q.E.D.
Proof: By $\langle 6\rangle 1$ and $\langle 6\rangle 2$; $po'_1$ is the $po'$ we are looking for.
$\langle 5\rangle 2.$ Case: $\langle 0, 1] \subseteq Q_1$
$\langle 6\rangle 1.$ Let: $o_2 \in [\![ d ]\!]^i$ s.t. $o_1 \rightsquigarrow_r o_2$
Proof: By assumption $\langle 3\rangle 1$ and Lemma 35
$\langle 6\rangle 2.$ Let: $o'_2 \in [\![ d' ]\!]^i$ s.t. $o_2 \rightsquigarrow_r o'_2$
Proof: By $\langle 6\rangle 1$ ($o_2 \in [\![ d ]\!]^i$) and assumption $\langle 1\rangle 1.3$
$\langle 6\rangle 3.$ Let: $Q'_2 \subseteq [0, 1]$ s.t. $(o'_2, Q'_2) \in [\![ g(d') ]\!]^p$
Proof: By $\langle 6\rangle 2$ and Lemma 34
$\langle 6\rangle 4.$ $po_1 \rightsquigarrow_{pr} po'_2$

⟨7⟩1. $o_1 \rightsquigarrow_r o'_2$

Proof: By ⟨6⟩1, ⟨6⟩2 and Lemma 26 in [HHRS06]

⟨7⟩2. $Q'_2 \subseteq Q_1$

⟨8⟩1. $0 \notin Q'_2$

Proof: By ⟨6⟩3 ($(o'_2, Q'_2) \in \llbracket\ g(d')\ \rrbracket^p$)

⟨8⟩2. Q.E.D.

Proof: By ⟨8⟩1 and assumption ⟨5⟩2

⟨7⟩3. Q.E.D.

Proof: By ⟨7⟩1 and ⟨7⟩2

⟨6⟩5. Q.E.D.

Proof: By ⟨6⟩4 and ⟨6⟩3; $po'_2$ is the $po'$ we are looking for

⟨5⟩3. Q.E.D.

Proof: By Lemma 32 the cases ⟨5⟩1 and ⟨5⟩2 are exhaustive

⟨4⟩2. Q.E.D.

Proof: ⇒-rule

⟨3⟩2. Q.E.D.

Proof: ∀-rule

⟨2⟩3. $\forall po' \in \llbracket\ g(d')\ \rrbracket^p : \exists S \subseteq \llbracket\ g(d')\ \rrbracket^p : \exists po \in \llbracket\ g(d)\ \rrbracket^p : po' \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨3⟩1. Assume: $po'_1 \in \llbracket\ g(d')\ \rrbracket^p$

Prove: $\exists S \subseteq \llbracket\ g(d')\ \rrbracket^p : \exists po \in \llbracket\ g(d)\ \rrbracket^p : po'_1 \in S \wedge po \rightsquigarrow_{pr} \bar{\oplus} S$

⟨4⟩1. Let: $(o_1, Q_1) \in \llbracket\ g(d)\ \rrbracket^p$ s.t. $Q_1 = \{1\}$

Proof: By Lemma 36

⟨4⟩2. $(o_1, Q_1) \rightsquigarrow_{pr} \bar{\oplus} \llbracket\ g(d')\ \rrbracket^p$

⟨5⟩1. Let: $o'_2 = \oplus \llbracket\ g(d')\ \rrbracket^p$

⟨5⟩2. $o_1 \rightsquigarrow_r o'_2$

⟨6⟩1. $\forall po \in \llbracket\ g(d)\ \rrbracket^p : o_1 \rightsquigarrow_r o$

Proof: By ⟨4⟩1 and Lemma 33

⟨6⟩2. $\bigcap_{(p,n) \in \llbracket\ d'\ \rrbracket^i} p \cup n = \bigcap_{((p,n),Q) \in \llbracket\ g(d')\ \rrbracket^p} p \cup n \wedge$
$\bigcap_{(p,n) \in \llbracket\ d'\ \rrbracket^i} n = \bigcap_{((p,n),Q) \in \llbracket\ g(d')\ \rrbracket^p} n$

Proof: By assumption ⟨1⟩1.1, ⟨2⟩1 and Lemma 39

⟨6⟩3. $p_1 \subseteq p'_2 \cup n'_2$

⟨7⟩1. $\forall po \in \llbracket\ g(d)\ \rrbracket^p : p_1 \subseteq p \cup n$

Proof: By ⟨6⟩1

⟨7⟩2. $\forall o \in \llbracket\ d\ \rrbracket^i : p_1 \subseteq p \cup n$

Proof: By ⟨7⟩1 and Lemma 34

⟨7⟩3. $\forall o' \in \llbracket\ d'\ \rrbracket^i : p_1 \subseteq p' \cup n'$

Proof: By ⟨7⟩2 and assumption ⟨1⟩1.3

⟨7⟩4. $p_1 \subseteq (\bigcup_{po \in \llbracket\ g(d')\ \rrbracket^p} p \cap \bigcap_{po \in \llbracket\ g(d')\ \rrbracket^p} p \cup n) \cup \bigcap_{po \in \llbracket\ g(d')\ \rrbracket^p} n$

⟨8⟩1. $p_1 \subseteq \bigcap_{(p,n) \in \llbracket\ d'\ \rrbracket^i} p \cup n$

Proof: By ⟨7⟩3

⟨8⟩2. $p_1 \subseteq \bigcap_{((p,n),Q) \in \llbracket\ g(d')\ \rrbracket^p} p \cup n$

Proof: By ⟨8⟩1 and ⟨6⟩2

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

Proof: By $\langle 8\rangle 2$

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

Proof: By $\langle 7\rangle 4$ and $\langle 5\rangle 1$

$\langle 6\rangle 4.$ $n_1 \subseteq n_2'$

$\langle 7\rangle 1.$ $\forall po \in [\![ \ g(d) \ ]\!]^p : n_1 \subseteq n$

Proof: By $\langle 6\rangle 1$

$\langle 7\rangle 2.$ $\forall o \in [\![ \ d \ ]\!]^i : n_1 \subseteq n$

Proof: By $\langle 7\rangle 1$ and Lemma 34

$\langle 7\rangle 3.$ $\forall o' \in [\![ \ d' \ ]\!]^i : n_1 \subseteq n'$

Proof: By $\langle 7\rangle 2$ and assumption $\langle 1\rangle 1.3$

$\langle 7\rangle 4.$ $n_1 \subseteq \bigcap_{((p,n),Q) \in [\![ \ g(d') \ ]\!]^p} n$

$\langle 8\rangle 1.$ $n_1 \subseteq \bigcap_{(p,n) \in [\![ \ d' \ ]\!]^i} n$

Proof: By $\langle 7\rangle 3$

$\langle 8\rangle 2.$ Q.E.D.

Proof: By $\langle 8\rangle 1$ and $\langle 6\rangle 2$

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

Proof: By $\langle 7\rangle 4$ and $\langle 5\rangle 1$

$\langle 6\rangle 5.$ Q.E.D.

Proof: By $\langle 6\rangle 3$ and $\langle 6\rangle 4$

$\langle 5\rangle 3.$ $\pi_2(\bar{\oplus}[\![ \ g(d') \ ]\!]^p) \subseteq Q_1$

$\langle 6\rangle 1.$ $\pi_2(\bar{\oplus}[\![ \ g(d') \ ]\!]^p) = \{1\}$

$\langle 7\rangle 1.$ $\exists (o', Q') \in [\![ \ g(d') \ ]\!]^p : Q' = \{1\}$

Proof: By Lemma 36

$\langle 7\rangle 2.$ $\forall (o', Q') \in [\![ \ g(d') \ ]\!]^p : Q' \neq \emptyset$

Proof: By Lemma 32

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

Proof: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and definition 7

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

Proof: By $\langle 6\rangle 1$ and $\langle 4\rangle 1$

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

Proof: By $\langle 5\rangle 2$ and $\langle 5\rangle 3$

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

Proof: By $\langle 4\rangle 1$ and $\langle 4\rangle 2$; $[\![ \ g(d') \ ]\!]^p$ is the $S$ we are looking for and $(o_1, Q_1)$ is the $po$ we are looking for

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

Proof: $\forall$-rule

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

Proof: By $\langle 2\rangle 2$ and $\langle 2\rangle 3$

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

Proof: $\Rightarrow$-rule

□

**Theorem 4. (Correspondence between $\rightsquigarrow_{nl}$ and $\rightsquigarrow_{pnl}$).** *Let $d$ and $d''$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$N(d) \wedge N(d') \wedge E(d') \wedge [\![ \ d \ ]\!]^i \rightsquigarrow_{nl} [\![ \ d' \ ]\!]^i \Rightarrow [\![ \ g(d) \ ]\!]^p \rightsquigarrow_{pnl} [\![ \ g(d') \ ]\!]^p$$

Proof.

```
⟨1⟩1. ASSUME: 1. $N(d)$
              2. $N(d')$
              3. $E(d')$
              4. $[\![ d ]\!]^i \rightsquigarrow_{nl} [\![ d' ]\!]^i$
      PROVE: $[\![ g(d) ]\!]^p \rightsquigarrow_{pnl} [\![ g(d') ]\!]^p$
  ⟨2⟩1. LET: $s \in \mathbb{P}(\mathcal{H}) : \forall (p,n) \in [\![ d' ]\!]^i : p \cup n = s$
    PROOF: By assumption ⟨1⟩1.2 and assumption ⟨1⟩1.3
  ⟨2⟩2. $\forall po \in [\![ g(d') ]\!]^p : p \cup n = s$
    ⟨3⟩1. LET: $s' \subseteq \mathcal{H}$ s.t. $\forall po \in [\![ g(d') ]\!]^p : p \cup n = s'$
      PROOF: By assumption ⟨1⟩1.3 and Lemma 43
    ⟨3⟩2. $s = s'$
      ⟨4⟩1. $\forall o \in [\![ d' ]\!]^i : p \cup n = s'$
        PROOF: By ⟨3⟩1 and Lemma 34
      ⟨4⟩2. Q.E.D.
        PROOF: By ⟨4⟩1 and ⟨2⟩1
    ⟨3⟩3. Q.E.D.
      PROOF: By ⟨3⟩1 and ⟨3⟩2
  ⟨2⟩3. $\forall po \in [\![ g(d) ]\!]^p : p \cup n = s$
    ⟨3⟩1. $\forall o \in [\![ d ]\!]^i : p \cup n = s$
      ⟨4⟩1. ASSUME: $o \in [\![ d ]\!]^i$
            PROVE: $p \cup n = s$
        ⟨5⟩1. LET: $o' \in [\![ d' ]\!]^i$ s.t. $o \rightsquigarrow_{nr} o'$
          PROOF: By assumption ⟨4⟩1 and assumption ⟨1⟩1.4
        ⟨5⟩2. $p' \cup n' = s$
          PROOF: By ⟨5⟩1 ($o' \in [\![ d' ]\!]^i$) and ⟨2⟩1
        ⟨5⟩3. Q.E.D.
          PROOF: By ⟨5⟩2 and ⟨5⟩1 ($o \rightsquigarrow_{nr} o'$)
      ⟨4⟩2. Q.E.D.
        PROOF: ∀-rule
    ⟨3⟩2. $E(d)$
      PROOF: By ⟨3⟩1 and assumption ⟨1⟩1.1
    ⟨3⟩3. LET: $s' \subseteq \mathcal{H}$ s.t. $\forall po \in [\![ g(d) ]\!]^p : p \cup n = s'$
      PROOF: By ⟨3⟩2 and Lemma 43
    ⟨3⟩4. $s = s'$
      ⟨4⟩1. $\forall o \in [\![ d ]\!]^i : p \cup n = s'$
        PROOF: By ⟨3⟩3 and Lemma 34
      ⟨4⟩2. Q.E.D.
        PROOF: By ⟨3⟩1 and ⟨4⟩1
    ⟨3⟩5. Q.E.D.
      PROOF: By ⟨3⟩3 and ⟨3⟩4
```

$\langle 2\rangle 4.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : 0 \notin Q \Rightarrow \exists po' \in \llbracket\ g(d')\ \rrbracket^p : po \rightsquigarrow_{pnr} po'$

$\langle 3\rangle 1.$ Assume: $po_1 \in \llbracket\ g(d)\ \rrbracket^p$

Prove: $0 \notin Q_1 \Rightarrow \exists po' \in \llbracket\ g(d')\ \rrbracket^p : po_1 \rightsquigarrow_{pnr} po'$

$\langle 4\rangle 1.$ Assume: $0 \notin Q_1$

Prove: $\exists po' \in \llbracket\ g(d')\ \rrbracket^p : po_1 \rightsquigarrow_{pnr} po'$

$\langle 5\rangle 1.$ Case: $Q_1 = \{1\}$

$\langle 6\rangle 1.$ Let: $po_1' \in \llbracket\ g(d')\ \rrbracket^p$ s.t. $Q_1' = \{1\}$

Proof: By Lemma 36

$\langle 6\rangle 2.$ $po_1 \rightsquigarrow_{pnr} po_1'$

$\langle 7\rangle 1.$ $o_1 \rightsquigarrow_r o_1'$

$\langle 8\rangle 1.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : o_1 \rightsquigarrow_r o$

Proof: By assumption $\langle 3\rangle 1$, assumption $\langle 5\rangle 1$ and Lemma 33

$\langle 8\rangle 2.$ $p_1 \subseteq p_1' \cup n_1'$

$\langle 9\rangle 1.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : p_1 \subseteq p \cup n$

Proof: By $\langle 8\rangle 1$

$\langle 9\rangle 2.$ $\forall o \in \llbracket\ d\ \rrbracket^i : p_1 \subseteq p \cup n$

Proof: By $\langle 9\rangle 1$ and Lemma 34

$\langle 9\rangle 3.$ $\forall o \in \llbracket\ d'\ \rrbracket^i : p_1 \subseteq p \cup n$

Proof: By $\langle 9\rangle 2$ and assumption $\langle 1\rangle 1.4$

$\langle 9\rangle 4.$ $\forall po \in \llbracket\ g(d')\ \rrbracket^p : p_1 \subseteq p \cup n$

Proof: By $\langle 9\rangle 3$, assumption $\langle 1\rangle 1.2$, $\langle 2\rangle 1$ and Lemma 39

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

Proof: By $\langle 9\rangle 4$ and $\langle 6\rangle 1$ ($po_1' \in \llbracket\ g(d')\ \rrbracket^p$)

$\langle 8\rangle 3.$ $n_1 \subseteq n_1'$

$\langle 9\rangle 1.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : n_1 \subseteq n$

Proof: By $\langle 8\rangle 1$

$\langle 9\rangle 2.$ $\forall o \in \llbracket\ d\ \rrbracket^i : n_1 \subseteq n$

Proof: By $\langle 9\rangle 1$ and Lemma 34

$\langle 9\rangle 3.$ $\forall o \in \llbracket\ d'\ \rrbracket^i : n_1 \subseteq n$

Proof: By $\langle 9\rangle 2$ and assumption $\langle 1\rangle 1.4$

$\langle 9\rangle 4.$ $\forall po \in \llbracket\ g(d')\ \rrbracket^p : n_1 \subseteq n$

Proof: By $\langle 9\rangle 3$, assumption $\langle 1\rangle 1.2$, $\langle 2\rangle 1$ and Lemma 39

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

Proof: By $\langle 9\rangle 4$ and $\langle 6\rangle 1$

$\langle 8\rangle 4.$ Q.E.D.

Proof: By $\langle 8\rangle 2$ and $\langle 8\rangle 3$

$\langle 7\rangle 2.$ $p_1 \cup n_1 = p_1' \cup n_1'$

$\langle 8\rangle 1.$ $p_1' \cup n_1' = s$

Proof: By $\langle 6\rangle 1$ and $\langle 2\rangle 2$

$\langle 8\rangle 2.$ $p_1 \cup n_1 = s$

Proof: By assumption $\langle 3\rangle 1$ and $\langle 2\rangle 3$

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

Proof: By $\langle 8\rangle 1$ and $\langle 8\rangle 2$

$\langle 7\rangle 3.$ $Q_1' \subseteq Q_1$

Proof: By assumption $\langle 5\rangle 1$ and $\langle 6\rangle 1$

$\langle 7\rangle 4.$ Q.E.D.

PROOF: By $\langle 7\rangle 1$, $\langle 7\rangle 2$ and $\langle 7\rangle 3$

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

PROOF: By $\langle 6\rangle 2$ and $\langle 6\rangle 1$; $po'_1$ is the $po'$ we are looking for.

$\langle 5\rangle 2.$ CASE: $\langle 0,1] \subseteq Q_1$

$\langle 6\rangle 1.$ $\exists o \in \llbracket\ d\ \rrbracket^i$ s.t. $o_1 \leadsto_{nr} o$

$\langle 7\rangle 1.$ LET: $o_2 \in \llbracket\ d\ \rrbracket^i$ s.t. $o_1 \leadsto_r o_2$

PROOF: By assumption $\langle 3\rangle 1$ and Lemma 35

$\langle 7\rangle 2.$ $o_1 \leadsto_{nr} o_2$

$\langle 8\rangle 1.$ $p_1 \cup n_1 = p_2 \cup n_2$

$\langle 9\rangle 1.$ $p_1 \cup n_1 = s$

PROOF: By assumption $\langle 3\rangle 1$ and $\langle 2\rangle 3$

$\langle 9\rangle 2.$ $p_2 \cup n_2 = s$

$\langle 10\rangle 1.$ $\exists Q \subseteq [0,1]$ s.t. $((p_2, n_2), Q) \in \llbracket\ g(d)\ \rrbracket^p$

PROOF: By $\langle 7\rangle 1$ and Lemma 34

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

PROOF: By $\langle 10\rangle 1$ $(((p_2, n_2), Q) \in \llbracket\ g(d)\ \rrbracket^p)$ and $\langle 2\rangle 3$

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

PROOF: By $\langle 9\rangle 1$ and $\langle 9\rangle 2$

$\langle 8\rangle 2.$ Q.E.D.

PROOF: By $\langle 7\rangle 1$ $(o_1 \leadsto_r o_2)$ and $\langle 8\rangle 1$

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

PROOF: By $\langle 7\rangle 1$ $(o_2 \in \llbracket\ d\ \rrbracket^i)$ and $\langle 7\rangle 2$; $o_2$ is the $o$ we are looking for

$\langle 6\rangle 2.$ LET: $o_2 \in \llbracket\ d\ \rrbracket^i$ s.t. $o_1 \leadsto_{nr} o_2$

PROOF: By $\langle 6\rangle 1$

$\langle 6\rangle 3.$ LET: $o'_2 \in \llbracket\ d'\ \rrbracket^i$ s.t. $o_2 \leadsto_{nr} o'_2$

PROOF: By $\langle 6\rangle 2$ $(o_2 \in \llbracket\ d\ \rrbracket^i)$ and assumption $\langle 1\rangle 1.4$

$\langle 6\rangle 4.$ LET: $Q'_2 \subseteq [0,1]$ s.t. $(o'_2, Q'_2) \in \llbracket\ g(d')\ \rrbracket^p$

PROOF: By $\langle 6\rangle 3$ and Lemma 34

$\langle 6\rangle 5.$ $po_1 \leadsto_{pnr} po'_2$

$\langle 7\rangle 1.$ $o_1 \leadsto_{nr} o'_2$

PROOF: By $\langle 6\rangle 2$, $\langle 6\rangle 3$ and Theorem 5

$\langle 7\rangle 2.$ $Q'_2 \subseteq Q_1$

$\langle 8\rangle 1.$ $0 \notin Q'_2$

PROOF: By $\langle 6\rangle 4$ $((o'_2, Q'_2) \in \llbracket\ g(d')\ \rrbracket^p)$ and Lemma 32

$\langle 8\rangle 2.$ Q.E.D.

PROOF: By $\langle 8\rangle 1$ and assumption $\langle 5\rangle 2$

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

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

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

PROOF: By $\langle 6\rangle 5$ and $\langle 6\rangle 4$; $po'_2$ is the $po'$ we are looking for

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

PROOF: By Lemma 32 the cases $\langle 5\rangle 1$ and $\langle 5\rangle 2$ are exhaustive

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

PROOF: $\Rightarrow$-rule

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

PROOF: $\forall$-rule

$\langle 2\rangle$5. $\forall po' \in \llbracket\, g(d')\,\rrbracket^p : \exists S \subseteq \llbracket\, g(d')\,\rrbracket^p : \exists po \in \llbracket\, g(d)\,\rrbracket^p : po' \in S \land po \rightsquigarrow_{pnr} \bar{\oplus} S$

$\langle 3\rangle$1. ASSUME: $po'_1 \in \llbracket\, g(d')\,\rrbracket^p$

PROVE: $\exists S \subseteq \llbracket\, g(d')\,\rrbracket^p : \exists po \in \llbracket\, g(d)\,\rrbracket^p : po'_1 \in S \land po \rightsquigarrow_{pnr} \bar{\oplus} S$

$\langle 4\rangle$1. LET: $(o_1, Q_1) \in \llbracket\, g(d)\,\rrbracket^p$ s.t. $Q_1 = \{1\}$

PROOF: By Lemma 36

$\langle 4\rangle$2. $(o_1, Q_1) \rightsquigarrow_{pnr} \bar{\oplus}\llbracket\, g(d')\,\rrbracket^p$

$\langle 5\rangle$1. LET: $o'_2 = \oplus\llbracket\, g(d')\,\rrbracket^p$

$\langle 5\rangle$2. $o_1 \rightsquigarrow_{nr} o'_2$

$\langle 6\rangle$1. $\forall po \in \llbracket\, g(d)\,\rrbracket^p : o_1 \rightsquigarrow_{nr} o$

$\langle 7\rangle$1. ASSUME: $po \in \llbracket\, g(d)\,\rrbracket^p$

PROVE: $o_1 \rightsquigarrow_{nr} o$

$\langle 8\rangle$1. $o_1 \rightsquigarrow_{r} o$

PROOF: By $\langle 4\rangle$1, assumption $\langle 7\rangle$1 and Lemma 33

$\langle 8\rangle$2. $p_1 \cup n_1 = p \cup n$

$\langle 9\rangle$1. $p_1 \cup n_1 = s$

PROOF: By $\langle 4\rangle$1 ($(o_1, Q_1) \in \llbracket\, g(d)\,\rrbracket^p$) and $\langle 2\rangle$3

$\langle 9\rangle$2. $p \cup n = s$

PROOF: By assumption $\langle 7\rangle$1 and $\langle 2\rangle$3

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

PROOF: By $\langle 8\rangle$1 and $\langle 8\rangle$2

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

PROOF: $\forall$-rule

$\langle 6\rangle$2. $\displaystyle\bigcap_{(p,n)\in\llbracket\, d'\,\rrbracket^i} p \cup n = \bigcap_{((p,n),Q)\in\llbracket\, g(d')\,\rrbracket^p} p \cup n \land$
$\displaystyle\bigcap_{(p,n)\in\llbracket\, d'\,\rrbracket^i} n = \bigcap_{((p,n),Q)\in\llbracket\, g(d')\,\rrbracket^p} n$

PROOF: By assumption $\langle 1\rangle$1.2, $\langle 2\rangle$1 and Lemma 39

$\langle 6\rangle$3. $p_1 \subseteq p'_2 \cup n'_2$

$\langle 7\rangle$1. $\forall po \in \llbracket\, g(d)\,\rrbracket^p : p_1 \subseteq p \cup n$

PROOF: By $\langle 6\rangle$1

$\langle 7\rangle$2. $\forall o \in \llbracket\, d\,\rrbracket^i : p_1 \subseteq p \cup n$

PROOF: By $\langle 7\rangle$1 and Lemma 34

$\langle 7\rangle$3. $\forall o' \in \llbracket\, d'\,\rrbracket^i : p_1 \subseteq p' \cup n'$

PROOF: By $\langle 7\rangle$2 and assumption $\langle 1\rangle$1.4

$\langle 7\rangle$4. $\displaystyle p_1 \subseteq (\bigcup_{po\in\llbracket\, g(d')\,\rrbracket^p} p \cap \bigcap_{po\in\llbracket\, g(d')\,\rrbracket^p} p \cup n) \cup \bigcap_{po\in\llbracket\, g(d')\,\rrbracket^p} n$

$\langle 8\rangle$1. $\displaystyle p_1 \subseteq \bigcap_{(p,n)\in\llbracket\, d'\,\rrbracket^i} p \cup n$

PROOF: By $\langle 7\rangle$3

$\langle 8\rangle$2. $\displaystyle p_1 \subseteq \bigcap_{((p,n),Q)\in\llbracket\, g(d')\,\rrbracket^p} p \cup n$

PROOF: By $\langle 8\rangle$1 and $\langle 6\rangle$2

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

PROOF: By $\langle 8\rangle$2

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

PROOF: By $\langle 7 \rangle 4$ and $\langle 5 \rangle 1$

$\langle 6 \rangle 4.$ $n_1 \subseteq n'_2$

$\langle 7 \rangle 1.$ $\forall po \in \llbracket\ g(d)\ \rrbracket^p : n_1 \subseteq n$

PROOF: By $\langle 6 \rangle 1$

$\langle 7 \rangle 2.$ $\forall o \in \llbracket\ d\ \rrbracket^i : n_1 \subseteq n$

PROOF: By $\langle 7 \rangle 1$ and Lemma 34

$\langle 7 \rangle 3.$ $\forall o' \in \llbracket\ d'\ \rrbracket^i : n_1 \subseteq n'$

PROOF: By $\langle 7 \rangle 2$ and assumption $\langle 1 \rangle 1.4$

$\langle 7 \rangle 4.$ $n_1 \subseteq \bigcap_{((p,n),Q) \in \llbracket\ g(d')\ \rrbracket^p} n$

$\langle 8 \rangle 1.$ $n_1 \subseteq \bigcap_{(p,n) \in \llbracket\ d'\ \rrbracket^i} n$

PROOF: By $\langle 7 \rangle 3$

$\langle 8 \rangle 2.$ Q.E.D.

PROOF: By $\langle 8 \rangle 1$ and $\langle 6 \rangle 2$

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

PROOF: By $\langle 7 \rangle 4$ and $\langle 5 \rangle 1$

$\langle 6 \rangle 5.$ $p'_2 \cup n'_2 = p_1 \cup n_1$

$\langle 7 \rangle 1.$ $p_1 \cup n_1 = s$

PROOF: By $\langle 4 \rangle 1$ and $\langle 2 \rangle 3$

$\langle 7 \rangle 2.$ $p'_2 \cup n'_2 = s$

PROOF: By $\langle 5 \rangle 1$ and $\langle 2 \rangle 2$

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

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

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

PROOF: By $\langle 6 \rangle 3$, $\langle 6 \rangle 4$ and $\langle 6 \rangle 5$

$\langle 5 \rangle 3.$ $\pi_2(\bar{\oplus}\llbracket\ g(d')\ \rrbracket^p) \subseteq Q_1$

$\langle 6 \rangle 1.$ $\pi_2(\bar{\oplus}\llbracket\ g(d')\ \rrbracket^p) = \{1\}$

$\langle 7 \rangle 1.$ $\exists (o', Q') \in \llbracket\ g(d')\ \rrbracket^p : Q' = \{1\}$

PROOF: By Lemma 36

$\langle 7 \rangle 2.$ $\forall (o', Q') \in \llbracket\ g(d')\ \rrbracket^p : Q' \neq \emptyset$

PROOF: By Lemma 32

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

PROOF: By $\langle 7 \rangle 1$, $\langle 7 \rangle 2$ and definition 7

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

PROOF: By $\langle 6 \rangle 1$ and $\langle 4 \rangle 1$

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

PROOF: By $\langle 5 \rangle 2$ and $\langle 5 \rangle 3$

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

PROOF: By $\langle 4 \rangle 1$ and $\langle 4 \rangle 2$; $\llbracket\ g(d')\ \rrbracket^p$ is the $S$ we are looking for and $(o_1, Q_1)$ is the $po$ we are looking for

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

PROOF: $\forall$-rule

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

PROOF: By $\langle 2 \rangle 4$ and $\langle 2 \rangle 5$

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

□

Lemma 58 and Lemma 59 show why stronger formulations of Theorem 3 do not hold. Lemma 60, Lemma 61 and Lemma 62 show why stronger/alternative formulations of Theorem 4 do not hold.

**Lemma 58.** *Let $d \in \mathcal{D}^i$. Then*

$$\llbracket\ d\ \rrbracket^i \rightsquigarrow_l \llbracket\ d'\ \rrbracket^i \not\Rightarrow \llbracket\ g(d)\ \rrbracket^p \rightsquigarrow_{pl} \llbracket\ g(d')\ \rrbracket^p$$

PROOF. Let

$$\begin{aligned} d &= aab \\ d_1 &= a \ \mathsf{xalt}\ aa \\ d_2 &= b \ \mathsf{alt}\ ab \\ d' &= d_1 \ \mathsf{seq}\ d_2 \end{aligned}$$

We then get

$$\begin{aligned} \llbracket\ d\ \rrbracket^i &= \{\ (\{\langle aab\rangle\}, \emptyset)\ \} \\ \llbracket\ d'\ \rrbracket^i &= \{\ (\{\langle ab\rangle, \langle aab\rangle\}, \emptyset), (\{\langle aab\rangle, \langle aaab\rangle\}, \emptyset)\ \} \end{aligned}$$

which means that $\llbracket\ d\ \rrbracket^i \rightsquigarrow_l \llbracket\ d'\ \rrbracket^i$. We also get

$$\begin{aligned} g(d) &= aab \\ g(d_1) &= a;\langle 0,1] \ \mathsf{palt}\ aa;\langle 0,1] \\ g(d_2) &= b \ \mathsf{alt}\ ab \\ g(d') &= g(d_1) \ \mathsf{seq}\ g(d_2) \end{aligned}$$

which means that

$$\begin{aligned} \llbracket\ g(d)\ \rrbracket^p &= \{\ ((\{\langle aab\rangle\}, \emptyset), \{1\})\} \\ \llbracket\ g(d_1)\ \rrbracket^p &= \{\ ((\{\langle a\rangle\}, \emptyset), \langle 0,1]), ((\{\langle aa\rangle\}, \emptyset), \langle 0,1]), ((\emptyset, \emptyset), \langle 0,1]), ((\emptyset, \emptyset), \{1\})\ \} \\ \llbracket\ g(d_2)\ \rrbracket^p &= \{\ ((\{\langle b\rangle, \langle ab\rangle\}, \emptyset), \{1\})\} \\ \llbracket\ g(d')\ \rrbracket^p &= \{\ ((\{\langle ab\rangle, \langle aab\rangle\}, \emptyset), \langle 0,1]), ((\{\langle aab\rangle, \langle aaab\rangle\}, \emptyset), \langle 0,1]), \\ &\qquad ((\emptyset, \emptyset), \langle 0,1]), ((\emptyset, \emptyset), \{1\})\ \} \end{aligned}$$

So $\llbracket\ g(d)\ \rrbracket^p \rightsquigarrow_{pl} \llbracket\ g(d')\ \rrbracket^p$ does not hold, because for every $S \subseteq \llbracket\ g(d')\ \rrbracket^p$ such that $((\emptyset, \emptyset), \{1\}) \in S$ we get $((\{\langle aab\rangle\}, \emptyset), \{1\}) \not\rightsquigarrow_{pr} \bar{\oplus} S$, since $\langle aab\rangle$ will be inconclusive in $\bar{\oplus} S$ for any such $S$.

□

**Lemma 59 (Non-correspondence).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$E(d) \wedge E(d') \wedge \llbracket\ d\ \rrbracket^i \rightsquigarrow_l \llbracket\ d'\ \rrbracket^i \not\Rightarrow \llbracket\ g(d)\ \rrbracket^p \rightsquigarrow_{pl} \llbracket\ g(d')\ \rrbracket^p$$

PROOF. Let

$$\begin{aligned} d &= \textsf{refuse } abc \\ d_1 &= (ab \textsf{ alt refuse } a) \textsf{ xalt } (a \textsf{ alt refuse } ab) \\ d_2 &= bc \textsf{ alt } c \\ d' &= d_1 \textsf{ seq } d_2 \end{aligned}$$

This means that $E(d)$ and $E(d')$ holds. We get

$$\begin{aligned} [\![\ d\ ]\!]^i &= \{\ (\emptyset, \{\langle abc\rangle\})\ \} \\ [\![\ d'\ ]\!]^i &= \{\ (\{\langle abc\rangle, \langle abbc\rangle\}, \{\langle ac\rangle, \langle abc\rangle\}), (\{\langle ac\rangle, \langle abc\rangle\}, \{\langle abc\rangle, \langle abbc\rangle\})\ \} \end{aligned}$$

which means that $[\![\ d\ ]\!]^i \rightsquigarrow_l [\![\ d'\ ]\!]^i$. We also get

$$\begin{aligned} g(d) &= \textsf{refuse } abc \\ g(d_1) &= (ab \textsf{ alt refuse } a);\langle 0,1] \textsf{ palt } (a \textsf{ alt refuse } ab);\langle 0,1] \\ g(d_2) &= bc \textsf{ alt } c \\ g(d') &= d_1 \textsf{ seq } d_2 \end{aligned}$$

which means that

$$\begin{aligned} [\![\ g(d)\ ]\!]^p &= \{\ ((\emptyset, \{\langle abc\rangle\}), \{1\})\} \\ [\![\ g(d_1)\ ]\!]^p &= \{\ ((\{\langle ab\rangle\}, \{\langle a\rangle\}), \langle 0,1]), ((\{\langle a\rangle\}, \{\langle ab\rangle\}), \langle 0,1]), \\ &\qquad ((\{\langle a\rangle, \langle ab\rangle\}, \emptyset), \langle 0,1]), ((\{\langle a\rangle, \langle ab\rangle\}, \emptyset), \{1\})\ \} \\ [\![\ g(d_2)\ ]\!]^p &= \{\ ((\{\langle bc\rangle, \langle c\rangle\}, \emptyset), \{1\})\} \\ [\![\ g(d')\ ]\!]^p &= \{\ ((\{\langle abc\rangle, \langle abbc\rangle\}, \{\langle ac\rangle, \langle abc\rangle\}), \langle 0,1]), \\ &\qquad ((\{\langle ac\rangle, \langle abc\rangle\}, \{\langle abc\rangle, \langle abbc\rangle\}), \langle 0,1]), \\ &\qquad ((\{\langle ac\rangle, \langle abc\rangle, \langle abbc\rangle\}, \emptyset), \langle 0,1]), ((\{\langle ac\rangle, \langle abc\rangle, \langle abbc\rangle\}, \emptyset), \{1\})\ \} \end{aligned}$$

So $[\![\ g(d)\ ]\!]^p \rightsquigarrow_{pl} [\![\ g(d')\ ]\!]^p$ does not hold, because for every $S \subseteq [\![\ g(d')\ ]\!]^p$ such that $((\{\langle ac\rangle, \langle abc\rangle, \langle abbc\rangle\}, \emptyset), \{1\}) \in S$ we get $((\emptyset, \{\langle abc\rangle\}), \{1\}) \not\rightsquigarrow_{pr} \bar{\oplus} S$, since $\langle abc\rangle$ will not be negative in $\bar{\oplus} S$ for any such $S$.

**Lemma 60 (Non-correspondence).** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$E(d) \wedge E(d') \wedge [\![\ d\ ]\!]^i \rightsquigarrow_{nl} [\![\ d'\ ]\!]^i \not\Rightarrow [\![\ g(d)\ ]\!]^p \rightsquigarrow_{pnl} [\![\ g(d')\ ]\!]^p$$

PROOF. The counter example is identical to the counter example for Lemma 59, except that we let $d = ac \textsf{ alt } (abbc \textsf{ alt } (\textsf{refuse } abc))$. This means that

$$[\![\ d\ ]\!]^i = \{\ (\{\langle ac\rangle, \langle abbc\rangle\}, \{\langle abc\rangle\})\ \}$$

and ensures that $[\![\ d\ ]\!]^i \rightsquigarrow_{nl} [\![\ d'\ ]\!]^i$ holds. □

**Lemma 61.** *Let $d \in \mathcal{D}^i$. Then*

$$\llbracket\ d\ \rrbracket^i \rightsquigarrow_{nl} \llbracket\ d'\ \rrbracket^i \not\Rightarrow \llbracket\ g(d)\ \rrbracket^p \rightsquigarrow_{pnl} \llbracket\ g(d')\ \rrbracket^p$$

Proof. This follows immediately from Lemma 60. We include the following counter example since it (unlike the counter example for Lemma 60) does not use a specification where a trace is both positive and negative in the same interaction obligation. Let

$$\begin{aligned} d &= (ab \ \mathsf{alt}\ aab)\ \mathsf{xalt}\ (aab\ \mathsf{alt}\ aaab) \\ d_1 &= a\ \mathsf{xalt}\ aa \\ d_2 &= b\ \mathsf{alt}\ ab \\ d' &= d_1\ \mathsf{seq}\ d_2 \end{aligned}$$

We then get

$$\begin{aligned} &\llbracket\ d\ \rrbracket^i = \{\ (\{\langle ab\rangle\,, \langle aab\rangle\}, \emptyset), (\{\langle aab\rangle\,, \langle aaab\rangle\}, \emptyset)\ \} \\ &\llbracket\ d'\ \rrbracket^i = \llbracket\ d\ \rrbracket^i \end{aligned}$$

which means that $\llbracket\ d\ \rrbracket^i \rightsquigarrow_{nl} \llbracket\ d'\ \rrbracket^i$. We also get

$$\begin{aligned} g(d) &= (ab\ \mathsf{alt}\ aab);\langle 0,1]\ \ \mathsf{palt}\ (aab\ \mathsf{alt}\ aaab);\langle 0,1] \\ g(d_1) &= a;\langle 0,1]\ \ \mathsf{palt}\ aa;\langle 0,1] \\ g(d_2) &= b\ \mathsf{alt}\ ab \\ g(d') &= g(d_1)\ \mathsf{seq}\ g(d_2) \end{aligned}$$

which means that

$$\begin{aligned} \llbracket\ g(d)\ \rrbracket^p &= \{\ ((\{\langle ab\rangle\,, \langle aab\rangle\}, \emptyset), \langle 0,1]), ((\{\langle aab\rangle\,, \langle aaab\rangle\}, \emptyset), \langle 0,1]), \\ &\qquad ((\{\langle aab\rangle\}, \emptyset), \langle 0,1]), ((\{\langle aab\rangle\}, \emptyset), \{1\})\ \} \\ \llbracket\ g(d_1)\ \rrbracket^p &= \{\ ((\{\langle a\rangle\}, \emptyset), \langle 0,1]), ((\{\langle aa\rangle\}, \emptyset), \langle 0,1]), ((\emptyset, \emptyset), \langle 0,1]), ((\emptyset, \emptyset), \{1\})\ \} \\ \llbracket\ g(d_2)\ \rrbracket^p &= \{\ ((\{\langle b\rangle\,, \langle ab\rangle\}, \emptyset), \{1\})\} \\ \llbracket\ g(d')\ \rrbracket^p &= \{\ ((\{\langle ab\rangle\,, \langle aab\rangle\}, \emptyset), \langle 0,1]), ((\{\langle aab\rangle\,, \langle aaab\rangle\}, \emptyset), \langle 0,1]), \\ &\qquad ((\emptyset, \emptyset), \langle 0,1]), ((\emptyset, \emptyset), \{1\})\ \} \end{aligned}$$

So $\llbracket\ g(d)\ \rrbracket^p \rightsquigarrow_{pl} \llbracket\ g(d')\ \rrbracket^p$ does not hold, because for every $S \subseteq \llbracket\ g(d')\ \rrbracket^p$ such that $((\emptyset, \emptyset), \{1\}) \in S$ we get $\bar{\oplus} S = ((\emptyset, \emptyset), \{1\})$, which gives $po \not\rightsquigarrow_{pnr} \bar{\oplus} S$ for all $po \in \llbracket\ d\ \rrbracket^p$.

**Lemma 62.** *Let $d$ and $d'$ be sequence diagrams in $\mathcal{D}^i$. Then*

$$N(d') \wedge E(d') \wedge \llbracket\ d\ \rrbracket^i \rightsquigarrow_{nl} \llbracket\ d'\ \rrbracket^i \not\Rightarrow \llbracket\ g(d)\ \rrbracket^p \rightsquigarrow_{pnl} \llbracket\ g(d')\ \rrbracket^p$$

Proof. Let

$$\begin{aligned} d_1 &= a\ \mathsf{xalt}\ aa \\ d_2 &= b\ \mathsf{alt}\ ab \\ d_3 &= ab\ \mathsf{alt}\ aaab \\ d &= (d_1\ \mathsf{seq}\ d_2)\ \mathsf{alt}\ d_3 \\ d' &= ab\ \mathsf{alt}\ (aab\ \mathsf{alt}\ aaab) \end{aligned}$$

Then $d'$ does not contain any $\mathsf{xalt}$ operator, so $N(d') \wedge E(d')$ is trivially fulfilled. Furthermore, we get

$$[\![\ d\ ]\!]^i = [\![\ d'\ ]\!]^i = \{\ (\{\langle ab\rangle, \langle aab\rangle, \langle aaab\rangle\}, \emptyset)\ \}$$

which means that $[\![\ d\ ]\!]^i \rightsquigarrow_{nl} [\![\ d'\ ]\!]^i$ holds. But in the probabilistic case we get

$$\begin{aligned}
[\![\ g(d_1)\ ]\!]^p &= \{\ ((\{\langle a\rangle\}, \emptyset), \langle 0, 1]), ((\{\langle aa\rangle\}, \emptyset), \langle 0, 1]),\\
&\qquad ((\emptyset, \emptyset), \langle 0, 1]), ((\emptyset, \emptyset), \{1\})\ \}\\
[\![\ g(d_1 \ \mathsf{seq}\ d_2)\ ]\!]^p &= \{\ ((\{\langle ab\rangle, \langle aab\rangle\}, \emptyset), \langle 0, 1]), ((\{\langle aab\rangle, \langle aaab\rangle\}, \emptyset), \langle 0, 1]),\\
&\qquad ((\emptyset, \emptyset), \langle 0, 1]), ((\emptyset, \emptyset), \{1\})\ \}\\
[\![\ g(d)\ ]\!]^p &= \{\ ((\{\langle ab\rangle, \langle aab\rangle, \langle aaab\rangle\}, \emptyset), \langle 0, 1]),\\
&\qquad ((\{\langle ab\rangle, \langle aaab\rangle\}, \emptyset), \langle 0, 1]), ((\{\langle ab\rangle, \langle aaab\rangle\}, \emptyset), \{1\})\ \}\\
[\![\ g(d')\ ]\!]^p &= \{\ ((\{\langle ab\rangle, \langle aab\rangle, \langle aaab\rangle\}, \emptyset), \{1\})\ \}
\end{aligned}$$

This means that $[\![\ g(d)\ ]\!]^p \rightsquigarrow_{pnl} [\![\ g(d')\ ]\!]^p$ does not hold, since the p-obligations in $[\![\ g(d)\ ]\!]^p$ where $\langle aab\rangle$ is inconclusive are not represented in $[\![\ g(d')\ ]\!]^p$.