Vicious circles in contracts and in logic☆

Massimo Bartoletti*, Tiziana Cimoli, Paolo Di Giamberardino

Dipartimento di Matematica e Informatica, Università degli Studi di Cagliari, Italy

Roberto Zunino

Dipartimento di Matematica, Università degli Studi di Trento, Italy

Abstract

Contracts are formal promises on the future interactions of participants, which describe the causal dependencies among their actions. An inherent feature of contracts is that such dependencies may be circular: for instance, a buyer promises to pay for an item if the seller promises to ship it, and vice versa. We establish a bridge between two formal models for contracts, one based on games over event structures, and the other one on Propositional Contract Logic. In particular, we show that winning strategies in the game-theoretic model correspond to proofs in the logic.

Keywords: contracts, propositional contract logic, event structures

1. Introduction

Contracts are formal descriptions of the behaviour of programs or services, used in the software development process to maintain consistency between specification and implementation. Contracts have recently gained an increasing relevance in the design and implementation of concurrent and distributed systems, as advocated e.g. by the OASIS reference model for service-oriented architectures [1]. This interest is witnessed by the proliferation of formal systems for contracts that appeared in the literature in the last few years. Such formalisms have been devised by adapting and extending models of concurrent systems, such as Petri nets [2, 3], event structures [4, 5], process algebras [6, 7, 8, 9, 10], timed automata [11, 12], and by extending various logics, such as modal [13], intuitionistic [14, 15], linear [14], and deontic [16, 17] logics (just to cite a few recent approaches). On a more applied side, tools have been developed to put some of such formalisms in practice. For instance, Scribble [18] can be used to specify the overall interaction protocol (named *choreography*) of a distributed application formed by a set of communicating services. By projecting such a choreography on each of these services [10], we obtain the specification of the interaction behaviour expected from each single service involved in the application. These projections have the form of *session types* [19, 20], i.e. contracts which regulate the inputs/outputs each service is expected to perform. Scribble allows the designer of a distributed application to verify properties of the choreography (e.g. the absence of deadlocks), and to automatically construct monitors ensuring that each service participating in the application respects its contract [21].

A main motivation for using contracts lies in that large distributed applications are typically constructed by composing services published by different organizations. The larger an application is, the greater the probability that some of its components deviates from the expected behaviour (either because of unintentional bugs, or maliciousness of a competing organisation). Hence, it becomes crucial to protect oneself

☆Work partially supported by Aut. Region of Sardinia under grants L.R.7/2007 CRP-17285 (TRICS), P.I.A. 2010 Project "Social Glue", by MIUR PRIN 2010-11 project "Security Horizons", and by EU COST Action IC1201 (BETTY).

* *Corresponding author.* Dipartimento di Matematica e Informatica, Università degli Studi di Cagliari, via Ospedale 72, 09124 Cagliari (Italy), e-mail: bart@unica.it

from other services' misbehaviour. Standard enforcement mechanisms (e.g., execution monitoring, static analysis, and model checking techniques) do not apply because of the total lack of control on code run by mutually untrusted, distributed services. Contracts may offer protection by legally binding services to behave as prescribed, or otherwise be blamed for a contract breach [22].

When contracts are used to support the reliability of distributed applications, the choice of the contract model (i.e. the formalism used to express and reason about contracts) is critical; just to give an example, assuming or not the trustworthiness of service brokers [23] (i.e. the entities which compose services) affects the kind of properties enforceable in different contract models [24]. To drive software architects in the choice of the most suitable contract model for novel applications, it would be desirable to clearly establish the actual properties and the relations among different models. This is not an easy task, because the constellation of formalisms proposed in the literature is wide and heterogeneous, and most works focus on studying a single formalism, rather than developing comparisons between different ones.

1.1. Vicious circles in contracts and in logic

In this paper, we relate two recent models for contracts — one based on game-theoretic notions and the other one on logic.

The game-theoretic model we consider was originally introduced in [24], and it is based on event structures (ES) [25]. The model assumes a set of *participants* (abstractions of services), who promise through their contracts to perform some *events*. These promises can be formalised as *enablings* of the form $X \vdash e$, meaning that an event e must be performed once all the events in the set X have been performed. For instance, consider a system composed by two participants, Alice (A) and Bob (B), associated with two events a and b, respectively, and assume that A is promising to fire a, while B is promising to fire b only after a has happened. Such promises are formalised by two ES with the following enablings:

$$\emptyset \vdash a \qquad\qquad \{a\} \vdash b \tag{1}$$

Contracts also define the goals of participants, in terms of a *payoff function* which associates each sequence of events with one of three outcomes: positive, negative, or neutral. In our Alice-Bob example, the payoff of A is positive in the sequences where she obtains b (i.e. b, ab, ba), negative in those where a is done while b is not, and neutral in the empty sequence. The payoffs of B are similar, with the role of a and b inverted.

The interaction among participants is modelled as a concurrent game [26], where participants "play" by performing events, trying to reach their goals. Each participant plays according to some strategy; roughly, a strategy is *winning* for a participant A if it allows A to fulfil her goals (i.e. reach a positive payoff) in all possible plays conforming to such strategy, and such that the other participants have no *obligations* (i.e. enabled events not yet performed). In our Alice-Bob example (1), a possible strategy for A would be just to fire a, and one for B would be to fire b once a has happened. These strategies are winning for both A and B: roughly, the only play conforming to such strategies where no one has pending obligations is ab, and in such play both participants have reached their goals.

Two key notions in this model are *agreement* and *protection*. Intuitively, a set of contracts has the agreement property whenever each participant has a winning strategy. Instead, protection is the property of the contract of a single participant A ensuring that, whenever she interacts with others (possibly adversaries), she has at least one strategy guaranteeing non-negative payoffs in plays without pending promises. The contracts in (1) admit an agreement, but A is *not* protected by her contract. Indeed, when the contract of A interacts with a contract which promises nothing, in all the plays where A has no pending promises (i.e. where she has performed a) her payoff is negative, regardless of her strategy.

When promises are modelled as Winskel's ES [25], it is shown in [24] that agreement and protection cannot hold at the same time. To give an intuition of why they are mutually exclusive, consider the following variation of the Alice-Bob contracts: A, which was not protected in (1), now requires b to happen before a.

$$\{b\} \vdash a \qquad\qquad \{a\} \vdash b \tag{2}$$

The contracts in (2) protect both A and B, but they do *not* enjoy the agreement. Indeed, the only admissible play in (2) is the empty one, because of the *vicious circle* determined by the mutual dependency between the two events a and b.

The other model of contracts [15] we consider in this paper is based on intuitionistic propositional logic (IPC): promises are represented by logical formulae, and obligations are derived through the entailment relation of the logic. The kind of vicious circles described in (2) can also happen in the logic-based model. For instance, consider the following formula of intuitionistic propositional logic (IPC):

$$(a \to b) \wedge (b \to a) \tag{3}$$

which says that b is provable provided that one has a proof of a, and *vice versa*, a is provable through a proof of b. Because of the mutual dependency between a and b, it turns out that from (3) neither a nor b can be deduced in the proof system of IPC.

1.2. From vicious to virtuous circles

To reconcile agreements with protection, an extension of ES called *event structures with circular causality* (CES for short) has been proposed in [5]. CES extend ES with a further enabling relation $\Vdash$, which allows to decouple conditional promises (e.g., doing e in exchange of X) from the temporal order in which events are performed. Having the Alice-Bob example in mind, $\{b\} \Vdash a$ means that "Alice will do a if Bob will *eventually* do b". This contract protects A, and it turns the vicious circle into a *virtuous* circle: indeed, when the contract of A interacts with the contract $\{a\} \vdash b$ of B, a winning strategy for A allows her to fire a at the first step, which causes an obligation for B to do b. Therefore, the composition of the contracts of A and B admits an agreement. In general, in [24] a technique is proposed which synthesises a set of contracts from the participants payoffs enjoying both agreement and protection.

In the logic-based contract model, virtuous circles are obtained by extending IPC with a "contractual" form of implication (denoted by $\twoheadrightarrow$); this extension is called propositional contract logic (PCL [15]). The intuition is that a formula $p \twoheadrightarrow q$ entails q not only when p is provable, but also in the case that a "compatible" formula is assumed. This compatible formula can take different forms, but the archetypal example is the (somewhat dual) $q \twoheadrightarrow p$. While:

$$(p \to q) \wedge (q \to p) \;\to\; p \wedge q$$

is *not* a theorem of IPC (because of the vicious circle), we have that

$$(p \twoheadrightarrow q) \wedge (q \twoheadrightarrow p) \;\to\; p \wedge q$$

is a theorem of PCL, because, similarly to $\Vdash$ in CES, $\twoheadrightarrow$ turns vicious into virtuous circles.

The meaning of contractual implication is clarified by comparing the natural deduction rule of elimination of $\to$ in IPC with the rule of elimination of $\twoheadrightarrow$ in PCL:

$$\frac{\Delta \vdash p \to q \qquad \Delta \vdash p}{\Delta \vdash q}\ (\to\mathrm{E}) \qquad\qquad \frac{\Delta \vdash p \twoheadrightarrow q \qquad \Delta, q \vdash p}{\Delta \vdash q}\ (\twoheadrightarrow\mathrm{E})$$

The two rules only differ in the context used to deduce the antecedent p: rule $(\twoheadrightarrow\mathrm{E})$ also allows for using as hypothesis the consequence q. Intuitively, adding q to the hypotheses Δ allows to break vicious circles, making it easier to deduce p, and in turn to eliminate $\twoheadrightarrow$. This is exemplified in the proof (4) below.

We can observe that both these models allow for a form of "circular" assume-guarantee reasoning. In our Alice-Bob example, assume that A promises to do a provided that she receives b in exchange, and B promises to do b in exchange of a. If we model these promises by a CES with enablings $\{b\} \Vdash a$ and $\{a\} \Vdash b$, then this contract enjoys agreement. The winning strategies of A and B consist in doing their events, without waiting for the other to take the first step; these strategies lead to a play where both a and b are performed (in any order). In PCL, the same scenario is represented by the theory $\Delta = b \twoheadrightarrow a,\ a \twoheadrightarrow b$, which entails both a and b. For instance, a proof of $\Delta \vdash a$ is the following (that of $\Delta \vdash b$ is symmetrical):

$$\dfrac{\Delta \vdash b \twoheadrightarrow a \qquad \dfrac{\Delta, a \vdash a \twoheadrightarrow b \quad \Delta, a, b \vdash a}{\Delta, a \vdash b}\ (\twoheadrightarrow\mathrm{E})}{\Delta \vdash a}\ (\twoheadrightarrow\mathrm{E}) \tag{4}$$

Note that the provable atoms (in the PCL theory Δ) are exactly the events occurring in a play where both participants win. This connection is not incidental: indeed, in Theorem 4.2 we will show that, for a certain class of contracts, agreement can be characterised in terms of provability in a PCL theory corresponding to the contract. In particular, in the presence of an agreement, all winning plays conforming to the winning strategy will contain all the provable atoms in the PCL theory.

The correspondence between contracts and PCL theories can be further refined. The insight is that each proof in a Horn PCL theory naturally induces a set of sequences (called *proof traces*) among the atoms. For instance, consider the theory $\Delta = a,\ a \to b$, which entails both a and b. In a proof of $\Delta \vdash a$, the only induced trace is a, since b is not needed. In a proof of $\Delta \vdash b$, to use the elimination rule of $\to$ one must first construct a proof of a, hence the only trace induced is ab. Summing up, the traces induced by Δ are all the sequences over a and b where, if b occurs, then a precedes it. Instead, the theory $\Delta = b \twoheadrightarrow a,\ a \twoheadrightarrow b$ induces both traces ab and ba. Proof traces correspond, in the realm of contracts, to the *prudent plays* where all participants perform all and only those events which are guaranteed to have a causal justification (possibly in the future). For instance, in the CES with enablings $\{b\} \Vdash a$ and $\{a\} \Vdash b$, we have that both plays ab and ba (corresponding to the proof traces of Δ) are prudent.

1.3. Contribution

Our main contributions can be summarised as follows:

- Theorem 4.2 shows that agreement in a class of game-theoretic contracts can be characterised in terms of provability in Horn PCL theories, and *vice versa*.
- Theorem 4.8 shows that proof traces in PCL correspond to prudent plays in contracts.
- Theorem 4.11 establishes that, whenever a contract admits an agreement, proof traces can be transformed into winning strategies for all participants.

The proofs of all our statements are contained either in the main body of the paper, or in Appendices A,B.

2. Game-theoretic contracts

We briefly review the theory of contracts introduced in [24]. Intuitively, a contract is a concurrent system featuring *obligations* (what a participant must do in a given state) and *objectives* (what a participant wishes to obtain in a given state). Obligations are modelled as event structures with circular causality (CES). A comprehensive account of CES is in [27]; here we shall only recall the necessary definitions. Assume given a denumerable universe of atomic actions $a, b, e, \ldots \in E$, called *events*, uniquely associated to *participants* $\mathsf{A}, \mathsf{B}, \ldots \in \mathcal{A}$ by a function $\pi : E \to \mathcal{A}$.

Definition 2.1 (CES). *A* CES $\mathcal{E}$ *is a triple* $\langle \#, \vdash, \Vdash \rangle$*, where*

- $\# \subseteq E \times E$ *is an irreflexive and symmetric* conflict *relation;*
- $\vdash \subseteq \mathit{Con} \times E$ *is the* enabling *relation;*
- $\Vdash \subseteq \mathit{Con} \times E$ *is the* circular enabling *relation.*

where:

- *for a set* $X \subseteq E$*, the predicate* $CF(X)$ *is true iff* X *is* conflict-free*, i.e.* $\forall e, e' \in X : \neg(e \# e')$*;*
- Con *is the set* $\{X \subseteq_{\mathit{fin}} E \mid CF(X)\}$*;*
- *the relations* $\vdash$ *and* $\Vdash$ *are* saturated*:* $\forall X \subseteq Y \subseteq_{\mathit{fin}} E.\ X \triangleright e \wedge CF(Y) \implies Y \triangleright e$*, for* $\triangleright \in \{\vdash, \Vdash\}$*.*

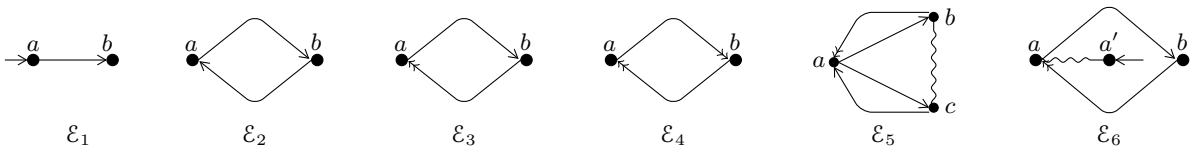

Figure 1: Graphical representation of CES. An edge from node a to node b denotes an enabling $\{a\} \triangleright b$, where $\triangleright$ is $\vdash$ if the edge has a single arrow, and $\triangleright$ is $\Vdash$ if it has a double arrow. A conflict $a\#b$ is represented by a wavy line between a and b. We will use hyperedges to represent enablings of the form $X \triangleright e$, when X is not a singleton.

A CES is *finite* when E is finite; it is *conflict-free* when the relation $\#$ is empty. We write $a \vdash b$ for $\{a\} \vdash b$, and $\vdash e$ for $\emptyset \vdash e$ (similar shorthands apply for $\Vdash$).

Intuitively, an enabling $X \vdash e$ models the fact that, if all the events in X have happened, then e is an obligation for participant $\pi(e)$; such obligation may be discharged only by performing e, or any event in conflict with e. For instance, an internal choice between a and b is modelled by a CES with enablings $\vdash a, \vdash b$ and conflict $a\#b$. After the choice (say, of a), the obligation b is discharged. The case of circular enablings $X \Vdash e$ is more complex, and it requires further notions; so we defer its precise treatment after Definition 2.12. Roughly, $X \Vdash e$ means that e is an event which can be done "on credit". Such credit will then be *honoured* when all the events in X are performed.

Besides the obligations, the other component of a contract is a function Φ which specifies the objectives of each participant. More precisely, Φ associates each participant A with a set of sequences in E^∞ (the set of finite or infinite sequences on E), which represent those executions where A has a positive payoff.

Definition 2.2 (Contract)**.** *A contract $\mathcal{C}$ is a pair $\langle \mathcal{E}, \Phi \rangle$, where $\mathcal{E}$ is a* CES*, and $\Phi : \mathcal{A} \to \wp(E^\infty)$.*

We interpret a contract as a nonzero-sum concurrent multi-player game [26]. The game involves the players in concurrently performing actions in order to reach their objectives.

Definition 2.3 (Play)**.** *A* play *of a contract $\mathcal{C}$ is a conflict-free sequence $\sigma \in E^\infty$ without repetitions.*

Notation 2.4. *For a sequence $\sigma = \langle e_0\, e_1 \cdots \rangle \in E^\infty$, we write $\overline{\sigma}$ for the set of events in σ; for all $i \leq |\sigma|$, we write σ_i for the subsequence $\langle e_0 \cdots e_{i-1} \rangle$. If $\sigma = \langle e_0 \cdots e_n \rangle$, we write $\sigma\, e$ for $\langle e_0 \cdots e_n\, e \rangle$. We denote the empty sequence by ε (hence we have $\sigma_0 = \varepsilon$ for all σ).*

Each play $\sigma = \langle e_0 \cdots e_i \cdots \rangle$ uniquely determines a computation:

$$(\emptyset, \emptyset) \xrightarrow{e_0} (\overline{\sigma_1}, \Gamma(\sigma_1)) \cdots \xrightarrow{e_i} (\overline{\sigma_{i+1}}, \Gamma(\sigma_{i+1})) \cdots$$

in the CES $\mathcal{E}$. The first element of each pair is the set of events occurred so far; the second element is the least set of events done "on credit", i.e. performed in the absence of a causal justification. Formally, for all sequences $\eta = \langle e_0\, e_1 \cdots \rangle$, we define $\Gamma(\eta) = \{e_i \in \overline{\eta} \mid \overline{\eta_i} \not\vdash e_i \ \wedge\ \overline{\eta} \not\Vdash e_i\}$. Notice that $e \notin \Gamma(\eta)$ iff either e is $\vdash$-enabled by the past events $\overline{\eta_i}$, or it is $\Vdash$-enabled by the *whole* play.

Example 2.5. *Consider the five* CES *in Figure 1. The maximal plays of $\mathcal{E}_1$–$\mathcal{E}_4$ are $\langle ab \rangle$, $\langle ba \rangle$, for which we have the following computations:*

$\mathcal{E}_1$: $(\emptyset,\emptyset) \xrightarrow{a} (\{a\},\emptyset) \xrightarrow{b} (\{a,b\},\emptyset)$ $\quad$ $(\emptyset,\emptyset) \xrightarrow{b} (\{b\},\{b\}) \xrightarrow{a} (\{a,b\},\{b\})$.

$\mathcal{E}_2$: $(\emptyset,\emptyset) \xrightarrow{a} (\{a\},\{a\}) \xrightarrow{b} (\{a,b\},\{a\})$ $\quad$ $(\emptyset,\emptyset) \xrightarrow{b} (\{b\},\{b\}) \xrightarrow{a} (\{a,b\},\{b\})$.

$\mathcal{E}_3$: $(\emptyset,\emptyset) \xrightarrow{a} (\{a\},\{a\}) \xrightarrow{b} (\{a,b\},\emptyset)$ $\quad$ $(\emptyset,\emptyset) \xrightarrow{b} (\{b\},\{b\}) \xrightarrow{a} (\{a,b\},\{b\})$.

$\mathcal{E}_4$: $(\emptyset,\emptyset) \xrightarrow{a} (\{a\},\{a\}) \xrightarrow{b} (\{a,b\},\emptyset)$ $\quad$ $(\emptyset,\emptyset) \xrightarrow{b} (\{b\},\{b\}) \xrightarrow{a} (\{a,b\},\emptyset)$.

The maximal plays of $\mathcal{E}_5$ are $\langle ab \rangle$, $\langle ba \rangle$, $\langle ac \rangle$, $\langle ca \rangle$. For $\langle ab \rangle$, $\langle ba \rangle$, the computations are as those of $\mathcal{E}_3$, while for $\langle ac \rangle$, $\langle ca \rangle$ the computations are as those of $\mathcal{E}_2$ (with c in place of b).

For all participants A, a *strategy* Σ for A is a function which associates to each finite play σ a set of events of A such that if $e \in \Sigma(\sigma)$ then σe is still a play. A play $\sigma = \langle e_0\, e_1 \cdots \rangle$ *conforms* to a strategy Σ for A if, for all $i \geq 0$, if $e_i \in \pi^{-1}(\mathsf{A})$, then $e_i \in \Sigma(\sigma_i)$; a strategy Σ has *past* η whenever η conforms to Σ.

Note that conformance to a strategy does not guarantee that all the events selected by such strategy are actually performed. For instance, consider the contract with enablings $\vdash a$, $\vdash b_0$ and $b_i \vdash b_{i+1}$ for all $i \in \mathbb{N}$, where a is an event of A and b_i are events of B. Here, the play $\eta = \langle b_0 b_1 \cdots \rangle$ conforms to the strategy of A defined by $\Sigma_{\mathsf{A}}(\sigma) = \{a\}$ when $a \notin \overline{\sigma}$, and $\Sigma_{\mathsf{A}}(\sigma) = \emptyset$ otherwise. Concretely, conformance only checks that *all* the events of A in the play (potentially none) agree with her strategy. As a further example, any (finite) prefix of η also conforms to Σ_{A}.

To define when a strategy Σ_{A} is winning, we will consider all and only those plays (conforming to Σ_{A}) in which the events chosen by Σ_{A} are eventually performed. As usual, this amounts to observing to *fair* plays. A play is *fair* w.r.t. a strategy Σ when there are no events in σ which are perpetually enabled by Σ.

Definition 2.6 (Fair play)**.** *A play $\sigma = \langle e_0\, e_1 \cdots \rangle$ is* fair *w.r.t. strategy Σ iff:*

$$\forall i \leq |\sigma|.\ \big(\forall j : i \leq j \leq |\sigma|.\ e \in \Sigma(\sigma_j)\big) \implies \exists h \geq i.\ e_h = e$$

We introduce below the crucial notion of prudent events, by slightly adapting the one in [24]. Since the formal definition is somehow elaborate, we start by providing the intuition underlying it, by first examining simpler definitions, which will turn out to be unsatisfactory. The idea is that an event e of a participant A is prudent in a certain play σ if, assuming the other participants fulfil their obligations, A can safely perform e. Here, "safely" concerns the possibility of doing e while being guaranteed that the events taken on credit after σ will be eventually honoured. If e is enabled by the events in σ (either via $\vdash$ or $\Vdash$), then it is prudent: indeed, credits will not increase by doing e. The non-trivial case is when e is instead $\Vdash$-enabled by some X *not* included in σ, since we do not know whether all the events in X will be eventually performed.

A first attempt at defining prudence could be the following:

Definition 2.7 (Prudence, tentative 1)**.** *An event e of A is prudent in σ whenever:*

$$\exists \eta\ :\ (\sigma, \Gamma(\sigma)) \xrightarrow{e\eta} (\sigma e \eta, \Gamma(\sigma e \eta)) \quad \wedge \quad \Gamma(\sigma e \eta) \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma)$$

Note that such definition implicitly considers non-deterministic choices as *angelic*, modelling a situation where all the participants cooperate to reach a common goal. Indeed, Definition 2.7 guarantees the existence of a play leading to a diminished credit set, and such behaviour intuitively is the one that will be followed in a cooperative setting. In other words, angelic non-determinism assumes that only the choices which lead to the goal are taken, so it does not capture the adversarial setting inherent to contracts, as the following example shows.

Example 2.8. *Assume the obligations of two participants A and B are modelled by the following event structure, where a_0, a_1, a_2 are the events of A, and b_0, b_1, b_2 are those of B:*

$$\begin{array}{llllll} b_2 \Vdash a_0 & b_0 \vdash a_1 & b_0 \vdash a_2 & b_1 \vdash a_2 & a_1 \# a_2 \\ a_0 \vdash b_0 & a_0 \vdash b_1 & a_1 \vdash b_2 & b_0 \# b_1 \end{array}$$

Here, a_0 is the only potential candidate for being a prudent event in the empty play, because all the other events have only $\vdash$-enablings. Assume that A fires a_0: then, B can internally choose between b_0 and b_1. If B fires b_1, then A must fire a_2. At this point, B is not obliged to fire b_2, because this would require the premise a_1, which is in conflict with the event a_2 done by A. Therefore, the credit a_0 will never be honoured in this play, and so a_0 has not to be considered prudent in the empty play. However, a_0 would be incorrectly classified prudent by Definition 2.7, because for $\eta = \langle b_0\, a_1\, b_2 \rangle$ we have that $\Gamma(a_0\eta) \cap \pi^{-1}(\mathsf{A}) = \emptyset \subseteq \Gamma(\varepsilon) = \emptyset$.

To address the issue raised by the previous example, we need to model *demonic* non-determinism, considering participants which compete to reach their goals. A naïve alternative definition could be the following:

Definition 2.9 (Prudence, tentative 2)**.** *An event e of A is prudent in σ whenever:*

$$\forall \eta \text{ maximal } : (\sigma, \Gamma(\sigma)) \xrightarrow{e\eta} (\sigma e\eta, \Gamma(\sigma e\eta)) \implies \Gamma(\sigma e\eta) \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma)$$

Unfortunately, this definition of prudence is still wrong, as witnessed by the following example:

Example 2.10. *Assume the obligations of two participants A and B are modelled by the following event structure, where a_0, a_1, a_2 are the events of A, and b_0, b_1, b_2 are those of B (notice that the only difference w.r.t. Example 2.8 is the last enabling of A, i.e. $b_1 \vdash a_1$):*

$$\begin{array}{llll} b_2 \Vdash a_0 & b_0 \vdash a_1 & b_0 \vdash a_2 & b_1 \vdash a_1 \quad a_1 \# a_2 \\ a_0 \vdash b_0 & a_0 \vdash b_1 & a_1 \vdash b_2 & b_0 \# b_1 \end{array}$$

As in Example 2.8, a_0 is the only potential candidate for being prudent in the empty play. After A has fired a_0, B can internally choose between b_0 and b_1. If B fires b_0, then A can choose between a_1 and a_2; by choosing a_1, A can make B fire b_2, so obtaining $\Gamma(\langle a_0 b_0 a_1 b_2 \rangle) = \emptyset$. If B fires b_1, then A can still fire a_1, after which B fires b_2. Also in this case, we obtain $\Gamma(\langle a_0 b_1 a_1 b_2 \rangle) = \emptyset$. Therefore, A can always drive her choices in order to make the credit a_0 honoured, and so a_0 can be considered prudent in the empty play. However, a_0 is incorrectly classified non-*prudent by Definition 2.9, because for $\eta = \langle b_0 a_2 \rangle$, which is a maximal extension of $\langle a_0 \rangle$, we have that $\Gamma(a_0\eta) \cap \pi^{-1}(\mathsf{A}) = \{a_0\} \not\subseteq \Gamma(\varepsilon) = \emptyset$.*

Here the problem is that, besides the choices of B, also those of A are considered demonic: indeed, even though it would be prudent for A to do a_0, the universal quantification over all plays η must consider also the play $\eta = \langle b_0 a_2 \rangle$, where A has chosen a_2. A correct definition of prudence must then consider an *alternating* form of determinism, where A tries to make credits honoured, while other participants play against.

As a further attempt towards a definition of prudence, consider the following one. To model angelic choices for A and demonic choices for the context, we allow A to choose her strategy Σ. Then, we restrict to *fair* plays, where A is always allowed to fire the events she has chosen through Σ.

Definition 2.11 (Prudence, tentative 3)**.** *A strategy Σ for A with past σ is* prudent *if, for all fair plays σ' extending σ and conforming to Σ:*

$$\exists k > |\sigma|.\ \Gamma(\sigma'_k) \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma)$$

An event e is prudent *in σ if there exists a prudent strategy Σ with past σ such that $e \in \Sigma(\sigma)$.*

As for the previous attempts, also this tentative definition is unsatisfactory: indeed in Example 2.10 the event a_0 is intuitively prudent in the empty play σ, while it is not according to Definition 2.11. To see why, assume that $a_0 \in \Sigma(\sigma)$, for some prudent strategy Σ for A. If we consider the extension $\sigma' = \langle a_0 \rangle$ of σ, we obtain (for $k = 1$, which is the only index we need to consider):

$$\Gamma(\sigma') \cap \pi^{-1}(\mathsf{A}) = \{a_0\} \not\subseteq \Gamma(\sigma) = \emptyset$$

and so we have that Σ is not prudent. Since this holds for all strategies Σ, Definition 2.11 would classify a_0 as *non*-prudent in $\sigma = \varepsilon$ — contradicting our intuition.

Here, the issue is that participant B did not perform any event in σ'. Intuitively, after a_0 is fired, either b_0 or b_1 are obligations for B, yet Definition 2.11 considers also those σ' where neither of these two events have been fired. This would model a strong form of demonic non-determinism, wherein B can chooses the worst option for A, including stopping himself. However, this would lead to an unsatisfactory notion of prudence, since no events of A $\Vdash$-enabled by events of the context (e.g. a_0 from the previous example) could ever be prudent. The desired notion of prudence would instead model demonic choices for the context where B can choose between different events, but he cannot stop doing obligations. For instance, in the previous example, since in σ' participant B does not respect his obligations, we should *not* consider σ' when checking whether a_0 is prudent. Because of this, we shall restrict the universal quantification of σ' to those plays in

which all other participants performed their obligations, and so are deemed *innocent*. The issue now involves properly defining the obligations of participants.

A first attempt at this would be requiring innocent participants to perform any event they can (also those "on credit"). However, this would require such participants to perform events "on credit" with no guarantee about whether they will be honoured. Such a requirement would be unrealistically asymmetric: after A makes a prudent move "on credit", she would expect others to honour such credit by performing their imprudent events, which may not ever be honoured. The correct definition would instead require other participants to perform their *prudent* events, only: this requires prudence and innocence to be *mutually* defined.

We finally arrive at the desired definition of prudence.

Definition 2.12 (Prudence)**.** *A strategy Σ for A with past σ is* prudent *if, for all fair plays σ' extending σ, conforming to Σ, and where all $\mathsf{B} \neq \mathsf{A}$ are innocent,*

$$\exists k > |\sigma|.\ \Gamma(\sigma'_k) \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma)$$

An event e is prudent *in σ if there exists a prudent strategy Σ with past σ such that $e \in \Sigma(\sigma)$.*
A participant A is innocent *in $\sigma = \langle e_0\, e_1 \cdots \rangle$ iff:*

$$\forall e \in \pi^{-1}(\mathsf{A}).\ \forall i \geq 0.\ \exists j \geq i.\ e \text{ is not prudent in } \sigma_j$$

If A is not innocent in σ, then she is culpable*.*

The definition of prudent strategies and of innocent participants is mutually coinductive (since we want to deal also with *infinite* plays). A participant A is considered *innocent* in a play σ when she has done all her prudent events in σ (hence, if a strategy tells A to do all her prudent events, then A is innocent in all conforming *fair* plays). Given a finite play σ of past events, an event e is *prudent* in σ whenever there exists a prudent strategy Σ which prescribes to do e in σ. A strategy for A with past σ (namely, conforming to σ) is prudent whenever, in all fair extensions of σ where all other participants are innocent, the events performed on credit by A are eventually honoured; at most, the credits coming from the past σ will be left. We neglect those *unfair* plays where an action permanently enabled is not eventually performed, since an unfair scheduler could perpetually prevent an honest participant from performing a promised action. Notice that the empty strategy is trivially prudent according to the definition above.

The definition of prudence involves mutually (co-)recursively defined entities. Further, it involves negations: e.g., innocence is defined in terms of non-prudent events. To ensure that the definition is indeed well-formed, it suffices to explicitly formalise prudence and innocence as the greatest fixed point of a monotonic function $F : L \to L$ for some complete lattice L, and apply Tarski's fixed point theorem. Our c.l. L is the product of the c.l. $(\wp(E \times E^*), \subseteq)$ (comprising relations such as "e is prudent in σ") and the c.l. $(\wp(\mathcal{A} \times E^\infty), \supseteq)$ (comprising relations such as "A is innocent in σ"). Hence, in our c.l. L we have $(P, I) \sqsubseteq_L (P', I')$ iff $P \subseteq P'$ and $I \supseteq I'$. Then, the function F underlying the definition of prudence is:

$$\begin{aligned}
F(P, I) &= (P', I') \qquad \text{where} \\
P' &= \{(e, \sigma) \mid \exists \Sigma.\ \sigma e \text{ conform to } \Sigma \wedge \\
&\qquad\qquad \forall \sigma' = \sigma\, e\, \eta \text{ fair conform to } \Sigma. \\
&\qquad\qquad\quad \big(\forall \mathsf{B} \neq \pi(e).\ (\mathsf{B}, \sigma') \in I\big) \implies \phi(\sigma, \sigma', \mathsf{A})\} \\
&\qquad \text{with } \phi(\sigma, \sigma', \mathsf{A}) \triangleq \exists k > |\sigma|.\ \Gamma(\sigma'_k) \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma) \\
I' &= \{(\mathsf{A}, \sigma) \mid \forall e \in \pi^{-1}(\mathsf{A}).\ \forall i \in 0..|\sigma|.\ \exists j \geq i.\ (e, \sigma_j) \notin P\}
\end{aligned}$$

It is straightforward to check that F is monotonic: roughly, increasing P makes I' smaller (while P' is unaffected), while decreasing I makes P' larger (while I' is unaffected).

Example 2.13. *Consider the obligations modelled by the five* CES *in Figure 1, where* $\pi(a) = \pi(a') = \mathsf{A}$ *and* $\pi(b) = \pi(c) = \mathsf{B}$*:*

- *in* $\mathcal{E}_1$*, the only prudent event in the empty play is* a*, which is enabled by* $\emptyset$*, and the only culpable participant is* A*. In* $\langle a \rangle$*,* b *becomes prudent, and* B *becomes culpable. In* $\langle ab \rangle$ *no event is prudent and no participant is culpable.*
- *in* $\mathcal{E}_2$*, there are no prudent events in* ε*. Instead, event* a *is prudent in* $\langle b \rangle$*, while* b *is prudent in* $\langle a \rangle$*: this is coherent with the fact that the prudence of an event does not depend on the assumption that all the events done in the past were prudent. In* $\langle ab \rangle$ *and* $\langle ba \rangle$ *no events are prudent.*
- *in* $\mathcal{E}_3$*, event* a *is prudent in* ε*: indeed, the only fair play* $a\eta$ *where* B *is innocent is* $\langle ab \rangle$*, where* $\Gamma(ab) = \emptyset$*. Instead,* b *is* not *prudent in* ε*, because* $b \in \Gamma(b\eta)$ *for all* η*. Event* b *is prudent in* $\langle a \rangle$*.*
- *in* $\mathcal{E}_4$*, both* a *and* b *are prudent in* ε*.*
- *in* $\mathcal{E}_5$*,* a *is* not *prudent in* ε*, because if* B *chooses to do* c*, then the credit* a *can no longer be honoured. Actually, no events are prudent in* ε*, while both* b *and* c *are prudent in* $\langle a \rangle$*, and* a *is prudent in both* $\langle b \rangle$ *and* $\langle c \rangle$*.*
- *in* $\mathcal{E}_6$*,* a *is prudent in* ε*, because after* a *has been fired,* B *must honour the credit by doing* b*. This example shows that prudent events are, in general, not persistent: an event which is prudent right now can become imprudent later on. In particular, if* A *chooses to fire* a' *in the empty play, then* a *is no longer prudent in the play* $\langle a' \rangle$*.*

We now provide the intuition about the obligations derived by an enabling $X \Vdash e$, by exploiting the notion of prudent events. Roughly, e is an obligation iff it is prudent, i.e. one can perform e "on credit", and nevertheless be guaranteed that in all possible executions of the contract, either the credit will be honoured (by doing the events in X), or the debtor will be culpable of a contract violation. For instance, in the contract with enablings $a \vdash b$ and $b \Vdash a$, the first enabling prescribes that b can be done after a, while the second enabling models the fact that a can be done on credit, on the guarantee that the other participant will be obliged to do b. The event a is prudent in the initial state, because after doing it the other participant has the obligation to perform b (not doing b will result in a violation).

We now define when a participant *wins* in a play. If A is culpable, then she loses. If A is innocent, but some other participant is culpable, then A wins. Otherwise, if all participants are innocent, then A wins if she has a positive payoff in the play, and the play is "credit-free".

Definition 2.14 (Winning play)**.** *Define the function* $\mathcal{W} : \mathcal{A} \to \wp(E^\infty)$ *as follows:*

$$\begin{aligned} \mathcal{W}\mathsf{A} = {} & \{\sigma \in \Phi\mathsf{A} \mid \mathsf{A} \textit{ is credit-free in } \sigma\textit{, and all participants are innocent in } \sigma\} \cup \\ & \{\sigma \mid \mathsf{A} \textit{ innocent in } \sigma\textit{, and some } \mathsf{B} \neq \mathsf{A} \textit{ is culpable in } \sigma\} \end{aligned}$$

where A *is* credit-free *in* σ *iff:* $\Gamma(\sigma) \cap \pi^{-1}(\mathsf{A}) = \emptyset$

Example 2.15. *Notice that innocence and credit-freeness are distinct notions. For instance, for the contract induced by the* CES $\mathcal{E}_3$ *in Figure 1, assuming* $\pi(a) = \mathsf{A}$ *and* $\pi(b) = \mathsf{B}$*, we have that in* $\sigma = \varepsilon$*,* A *is credit-free, but not innocent (because* a *is prudent in* ε*), in* $\sigma = \langle a \rangle$*,* A *is innocent, but not credit-free (because* $\Gamma(\langle a \rangle) = \{a\}$*), and in* $\sigma = \langle ab \rangle$*,* A *is innocent and credit-free.*

A key property of contracts is that of *agreement*. Intuitively, when A agrees on a contract $\mathcal{C}$, then she can safely initiate an interaction with the other participants, and be guaranteed that the interaction will not "go wrong" — even in the presence of attackers. This does not mean that A will always succeed in all interactions: in case B is dishonest, we do not assume that an external authority will dispossess B of b and give it to A. Participant A will agree on a contract where she reaches her goals, or she can blame another

participant for a contract violation. In real-world applications, a judge may provide compensations to A, or impose a punishment to the culpable participant.

We now define when a participant *agrees* on a contract. We say that Σ is *winning* for A iff A wins in every fair play which conforms to Σ. Intuitively, A is happy to participate in an interaction regulated by contract $\mathcal{C}$ when she has a strategy Σ which allows her to win in all fair plays conforming to Σ.

Definition 2.16 (Agreement)**.** *A participant* A agrees *on a contract* $\mathcal{C}$ *whenever* A *has a winning strategy in* $\mathcal{C}$*. A contract* $\mathcal{C}$ admits an agreement *whenever all the involved participants agree on* $\mathcal{C}$*.*

Example 2.17. *Consider the contracts* $\mathcal{C}_i$ *where the obligations are specified by* $\mathcal{E}_i$ *in Figure 1, and let the goals of* A *and* B *be as follows:* A *is happy when she obtains* b *(i.e.* $\Phi\mathsf{A} = \{\sigma \mid b \in \overline{\sigma}\}$*), while* B *is happy when he obtains* a *(*$\Phi\mathsf{B} = \{\sigma \mid a \in \overline{\sigma}\}$*).*

- $\mathcal{C}_1$ *admits an agreement. The winning strategies for* A *and* B *are, respectively,*

$$\Sigma_{\mathsf{A}}(\sigma) = \begin{cases} \{a\} & \text{if } a \notin \overline{\sigma} \\ \emptyset & \text{otherwise} \end{cases} \qquad \Sigma_{\mathsf{B}}(\sigma) = \begin{cases} \{b\} & \text{if } a \in \overline{\sigma} \text{ and } b \notin \overline{\sigma} \\ \emptyset & \text{otherwise} \end{cases}$$

  Roughly, the only fair play conforming to Σ_{A} *and* Σ_{B} *where both* A *and* B *are innocent is* $\sigma = \langle ab \rangle$*. We have that* A *and* B *win in* σ*, because both participants are credit-free in* σ *(see Example 2.5), and* $\sigma \in \Phi\mathsf{A} \cap \Phi\mathsf{B}$*.*

- $\mathcal{C}_2$ *does not admit an agreement. Indeed, there are no prudent events in* ε*, hence both* A *and* B *are innocent in* ε*. If no participant takes the first step, then nobody reaches her goals. If a participant takes the first step, then the resulting trace is not credit-free. Thus, no winning strategy exists.*

- $\mathcal{C}_3$ *admits an agreement. The winning strategies are as for* $\mathcal{C}_1$ *above:* A *first does* a*, then* B *does* b*. While* $\mathcal{C}_1$ *and* $\mathcal{C}_3$ *are identical from the point of view of agreements, they differ in that* $\mathcal{C}_3$ protects A*, while* $\mathcal{C}_1$ *does not. Intuitively, the enabling* $\vdash a$ *in* $\mathcal{C}_1$ *models an obligation for* A *also in those contexts where no agreement exists, while* $b \Vdash a$ *only forces* A *to do* a *when* b *is guaranteed.*

- $\mathcal{C}_4$ *admits an agreement. In this case the winning strategies for* A *and* B *are:*

$$\Sigma_{\mathsf{A}}(\sigma) = \begin{cases} \{a\} & \text{if } a \notin \overline{\sigma} \\ \emptyset & \text{otherwise} \end{cases} \qquad \Sigma_{\mathsf{B}}(\sigma) = \begin{cases} \{b\} & \text{if } b \notin \overline{\sigma} \\ \emptyset & \text{otherwise} \end{cases}$$

  That is, a participant must be ready to do her action without waiting for the other participant to make the first step.

- $\mathcal{C}_5$ *does not admit an agreement. Since no events are prudent in* ε*, both participants are innocent in* ε*, but they cannot reach their goals by doing nothing. If* A *does* a*, then* B *can choose to do* c*. This makes* B *innocent (and winning), but then* A *loses, because* A *is not credit-free in* $\langle ac \rangle$*.*

- $\mathcal{C}_6$ *does not admit an agreement. In particular,* A *agrees on* $\mathcal{C}_6$*, because she can choose to fire* a*, which is prudent and guarantees that* B *must do* b*. However,* B *does not agree on* $\mathcal{C}_6$*, because if* A *chooses to fire* a'*, then she will no longer be obliged to do* a*.*

The kind of payoff functions used in the previous example is quite common: the payoff is positive when some set of events have been done, neglecting the order in which events are actually fired. Informally, *reachability payoffs* are the functions Φ for which the order of events in a play σ is immaterial.

Definition 2.18. *Let* $\varphi : \mathcal{A} \to \wp(\wp(E))$*. We say that* $\Phi : \mathcal{A} \to \wp(E^\infty)$ *is* induced by φ *whenever* $\sigma \in \Phi\mathsf{A}$ *iff* $\overline{\sigma} \in \varphi(\mathsf{A})$*. A function* Φ *is a* reachability payoff *if it is induced by some* φ*.*

$$\frac{\Delta \vdash q}{\Delta \vdash p \twoheadrightarrow q}\ (\textsc{Zero}) \qquad \frac{\Delta,\ p \twoheadrightarrow q,\ p' \vdash p \quad \Delta,\ p \twoheadrightarrow q,\ q \vdash p' \twoheadrightarrow q'}{\Delta,\ p \twoheadrightarrow q \vdash p' \twoheadrightarrow q'}\ (\textsc{Lax}) \qquad \frac{\Delta,\ p \twoheadrightarrow q,\ r \vdash p \quad \Delta,\ p \twoheadrightarrow q,\ q \vdash r}{\Delta,\ p \twoheadrightarrow q \vdash r}\ (\textsc{Fix})$$

Figure 2: Sequent calculus for PCL (rules for $\twoheadrightarrow$; the full set of rules is in Figure 8).

$$\frac{}{\Delta, p \vdash p}\ (\textsc{Id}) \qquad \frac{\Delta \vdash p \qquad \Delta \vdash q}{\Delta \vdash p \wedge q}\ (\wedge\text{I}) \qquad \frac{\Delta \vdash p \wedge q}{\Delta \vdash p}\ (\wedge\text{E1}) \qquad \frac{\Delta \vdash p \wedge q}{\Delta \vdash q}\ (\wedge\text{E2})$$

$$\frac{\Delta \vdash p}{\Delta \vdash p \vee q}\ (\vee\text{I1}) \qquad \frac{\Delta \vdash q}{\Delta \vdash p \vee q}\ (\vee\text{I2}) \qquad \frac{\Delta \vdash p \vee q \qquad \Delta, p \vdash r \qquad \Delta, q \vdash r}{\Delta \vdash r}\ (\vee\text{E})$$

$$\frac{\Delta, p \vdash q}{\Delta \vdash p \to q}\ (\to\text{I}) \qquad \frac{\Delta \vdash p \to q \qquad \Delta \vdash p}{\Delta \vdash q}\ (\to\text{E})$$

$$\frac{\Delta \vdash q}{\Delta \vdash p \twoheadrightarrow q}\ (\twoheadrightarrow\text{I1}) \qquad \frac{\Delta \vdash p \twoheadrightarrow q \qquad \Delta, p' \vdash p \qquad \Delta, q \vdash p' \twoheadrightarrow q'}{\Delta \vdash p' \twoheadrightarrow q'}\ (\twoheadrightarrow\text{I2}) \qquad \frac{\Delta \vdash p \twoheadrightarrow q \qquad \Delta, q \vdash p}{\Delta \vdash q}\ (\twoheadrightarrow\text{E})$$

Figure 3: Natural deduction system for PCL.

3. Proof traces in Propositional Contract Logic

Propositional Contract Logic (PCL [15]) extends intuitionistic propositional logic (IPC) with the connective $\twoheadrightarrow$, called *contractual implication*. A proof system for PCL was introduced in [15] in terms of a Gentzen-style sequent calculus (Figure 2), which extends that of IPC. Decidability of PCL has been established in [15] following the lines of the proof of decidability of intuitionistic propositional logic given by Kleene in [28]. The result relies on a formulation of the PCL sequent calculus with implicit structural rules (to limit the proof search space of a given sequent, as in Kleene's G3 calculus) and the subformula property, obtained as consequence of the cut-elimination theorem.

The formulae $p, q, \ldots$ of PCL are defined as follows, where we assume that the set of atoms $a, b, \ldots$ coincides with the set of events E used in Section 2.

$$p, q \ ::= \ \bot \mid \top \mid a \mid \neg p \mid p \vee q \mid p \wedge q \mid p \to q \mid p \twoheadrightarrow q$$

A notable difference between contractual and intuitionistic implication is that the former allows for a form of *circular* reasoning, witnessed by the theorem of PCL:

$$(p \twoheadrightarrow q) \ \wedge \ (q \twoheadrightarrow p) \ \to \ p \ \wedge \ q \qquad \text{(THEOREM)}$$

whereas the following is *not* a theorem (neither of PCL nor of IPC):

$$(p \to q) \ \wedge \ (q \to p) \ \to \ p \ \wedge \ q \qquad \text{(NOT A THEOREM)}$$

3.1. Natural deduction for PCL

We introduce a natural deduction system for PCL, which we shall show equivalent to the sequent calculus of [15]. The natural deduction system for PCL extends that for IPC with the last three rules in Figure 3 (wherein, in all the rules, Δ is a set of PCL formulae). Provable formulae are contractually implied, according to rule ($\twoheadrightarrow$I1). Rule ($\twoheadrightarrow$I2) provides $\twoheadrightarrow$ with the same weakening properties of $\to$. The paradigmatic rule is ($\twoheadrightarrow$E), which allows for the elimination of $\twoheadrightarrow$. Compared to the rule ($\to$E) for elimination of $\to$ in IPC, the only difference is that in the context used to deduce the antecedent p, rule ($\twoheadrightarrow$E) also allows for using as hypothesis the consequence q.

Example 3.1. *Let $\Delta = a \to b, b \twoheadrightarrow a$. A proof of $\Delta \vdash a$ in natural deduction is the following:*

$$\dfrac{\Delta \vdash b \twoheadrightarrow a \qquad \dfrac{\Delta, a \vdash a \to b \qquad \overline{\Delta, a \vdash a}^{(\text{ID})}}{\Delta, a \vdash b}\ (\to\text{E})}{\Delta \vdash a}\ (\twoheadrightarrow\text{E})$$

The natural deduction system of Figure 3 is equivalent to the Gentzen calculus of [15].

Theorem 3.2. *$\Delta \vdash p$ is provable in natural deduction iff $\Delta \vdash p$ is provable in the sequent calculus of [15].*

The proof of Theorem 3.2 follows the lines of the proof of equivalence of natural deduction and sequent calculus given in [29]. The intuition is that right (resp. left) rules of the sequent calculus are represented in natural deduction by using introduction (resp. elimination) rules.

3.2. Horn fragment of PCL

In this paper we shall focus on the *Horn fragment* of PCL, which comprises atoms, conjunctions, and non-nested implications (both intuitionistic and contractual). This fragment is particularly insightful, because it has strong relations with the theory of contracts studied in Section 2, as we will show.

The Horn PCL fragment is defined below. It is the natural extension of its IPC counterpart, obtained by allowing both $\to$ and $\twoheadrightarrow$ arrows in clauses.

Definition 3.3 (Horn PCL theory)**.** *Let α, β range over n-ary conjunction of atoms $\bigwedge\{a_1, \ldots, a_n\}$ with $n \geq 0$, and let $\top$ denote $\bigwedge \emptyset$. A* Horn PCL theory *is a set of clauses of the form $\alpha \to a$ or $\alpha \twoheadrightarrow a$. We identify the atomic formula a with the clause $\top \to a$.*

For proving atoms (or their conjunctions) in Horn PCL theories, a strict subset of the natural deduction rules suffices.

Lemma 3.4. *Let Δ be a Horn* PCL *theory. If $\Delta \vdash \alpha$ in natural deduction, then a proof of $\Delta \vdash \alpha$ exists which uses only the rules* (ID)*,* ($\wedge$I)*,* ($\wedge$E1)*,* ($\wedge$E2)*,* ($\to$E)*, and* ($\twoheadrightarrow$E)*.*

3.3. Proof traces

Each Horn PCL theory Δ induces a set of atom orderings which are somehow "compatible" with the proofs having Δ as hypothesis. For instance, if Δ contains the clause $\alpha \to a$, then the elimination rule for $\to$ allows for the following proof:

$$\dfrac{\Delta \vdash \alpha \to a \qquad \Delta \vdash \alpha}{\Delta \vdash a}\ (\to\text{E})$$

The rule says that, to construct from Δ a proof of a, one first needs a proof of all the atoms in α. Therefore, if — as a *gedankenexperiment* — we collect in $[\![\Delta]\!]$ the set of all sequences of atoms "compatible" with the proofs in Δ, and if σ is a sequence in $[\![\Delta]\!]$ contaning all the atoms in α, then to be coherent with rule ($\to$E) we must also include σa in $[\![\Delta]\!]$. Hereafter, we shall refer to the sequences of atoms in $[\![\Delta]\!]$ as *proof traces*.

Consider now the elimination rule for $\twoheadrightarrow$:

$$\dfrac{\Delta \vdash \alpha \twoheadrightarrow a \qquad \Delta, a \vdash \alpha}{\Delta \vdash a}\ (\twoheadrightarrow\text{E})$$

Here, the intuition is that α needs not necessarily be proved before a: it suffices to prove α by taking a as hypothesis. Assuming that σ is a proof trace of Δ, a (i.e. Δ plus the hypothesis a), the proof traces of Δ must then include all the interleavings between σ and a.

In the rest of this section we formally define proof traces, and we study their properties. We begin by providing the needed notation.

Notation 3.5. *We denote with $\overline{\alpha}$ the set of atoms in α. For $\sigma, \eta \in E^*$, we denote with $\sigma\eta$ the concatenation of σ and η, and with $\sigma \mid \eta$ the set of interleavings of σ and η. We assume that both concatenation and interleaving operators remove duplicates from the right. For instance, $aba \mid ca = ab \mid ca = \{abc, acb, cab\}$.*

$$\frac{}{\varepsilon \in [\![\Delta]\!]}\,(\varepsilon) \qquad \frac{\alpha \to a \in \Delta \qquad \sigma \in [\![\Delta]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma}}{\sigma\, a \in [\![\Delta]\!]}\,(\to) \qquad \frac{\alpha \twoheadrightarrow a \in \Delta \qquad \sigma \in [\![\Delta, a]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma}}{\sigma \mid a \subseteq [\![\Delta]\!]}\,(\twoheadrightarrow)$$

Figure 4: Proof traces of Horn PCL.

To justify the removal of duplicates in a proof trace, remember that a proof trace in $[\![\Delta]\!]$ is an (ordered) sequence of atoms appearing in a derivation having Δ as hypothesis. Since PCL is a non-linear logic (where proving an atom once is the same as proving it several times) we just need to record the first occurence of it along a derivation.

Definition 3.6 (Proof traces)**.** *For a Horn* PCL *theory Δ, we define the set of sequences of atoms $[\![\Delta]\!]$ by the rules in Figure 4. We call each $\sigma \in [\![\Delta]\!]$ a* proof trace *of Δ.*

Note that the $\twoheadrightarrow$ rule carries a set inclusion in its consequence $\sigma \mid a \subseteq [\![\Delta]\!]$. This is just a convenient shorthand for adding a side condition $b \in (\sigma \mid a)$ and changing the conclusion to $b \in [\![\Delta]\!]$.

Also, note that a proof trace may be obtained through different derivations, and that a derivation can give rise to multiple proof traces (because of the interleaving operator).

Example 3.7. *Consider the following Horn* PCL *theories (recall that $a \triangleq \top \to a$):*

$$\Delta_1 = \{a \to b,\, a\} \qquad \Delta_2 = \{a \to b,\, b \to a\}$$
$$\Delta_3 = \{a \to b,\, b \twoheadrightarrow a\} \qquad \Delta_4 = \{a \twoheadrightarrow b,\, b \twoheadrightarrow a\}$$

(notice the resemblance with the CES *$\mathcal{E}_1$–$\mathcal{E}_4$ in Figure 1). By Definition 3.6, we have:*

$$[\![\Delta_1]\!] = \{\varepsilon,\, a,\, ab\} \qquad [\![\Delta_2]\!] = \{\varepsilon\}$$
$$[\![\Delta_3]\!] = \{\varepsilon,\, ab\} \qquad [\![\Delta_4]\!] = \{\varepsilon,\, ab,\, ba\}$$

For instance, we deduce $ab \in [\![\Delta_3]\!]$ through the following derivation:

$$\dfrac{b \twoheadrightarrow a \in \Delta_3 \qquad \dfrac{a \to b \in \Delta_3, a \qquad \dfrac{\top \to a \in \Delta_3, a \qquad \dfrac{}{\varepsilon \in [\![\Delta_3, a]\!]}\,(\varepsilon) \qquad \overline{\top} \subseteq \overline{\varepsilon}}{a \in [\![\Delta_3, a]\!]}\,(\to) \qquad \overline{a} \subseteq \overline{a}}{ab \in [\![\Delta_3, a]\!]}\,(\to) \qquad \overline{b} \subseteq \overline{ab}}{ab \in ab \mid a \subseteq [\![\Delta_3]\!]}\,(\twoheadrightarrow)$$

Notice that $ba \notin [\![\Delta_3]\!]$: indeed, to derive any non-empty α from Δ_3 one needs to use both $a \to b$ and $b \twoheadrightarrow a$, hence all non-empty proof traces must contain both a and b; since b does not occur at the right of a contractual implication, it cannot be interleaved; thus, ba is not derivable.

Note that the derivation in Example 3.7 follows the same steps of the one in Example 3.1. The use of rule (→E) is replaced by (→), while (↠E) is replaced by (↠). The (Id) rule is handled slightly differently, since we identify $a = \top \to a$ when dealing with Horn clauses, causing the use of (→) in the proof trace derivation, followed by (ε) on top. However, note that in general there is no direct correspondence between natural deduction proofs and derivations of proof traces, because rules (∧E1), (∧E2) and (∧I) have no counterparts in the inference rules for proof traces. Still, there does exist a correspondence between provability and proof traces, as stated in Lemma 3.11.

We now prove some basic properties of proof traces, which will be exploited later on in Section 3.4 and in Section 4, to relate proof traces with contracts. In all the statements below, Δ, Δ' are Horn PCL theories, while σ, η, ν are sequences of atoms (not necessarily proof traces).

The following lemma states that the operator $[\![\cdot]\!]$ is monotonic with respect to the inclusion relation between theories. This is straightforward by Definition 3.6.

Lemma 3.8. $\Delta \subseteq \Delta' \implies [\![\Delta]\!] \subseteq [\![\Delta']\!]$

Proof traces are closed under concatenation. Actually, the following lemma provides us with a stronger result: if σ is a proof trace of Δ, then we can append to σ any proof trace η which may also use (in addition to Δ) the atoms in σ as hypotheses.

Lemma 3.9. $\sigma \in [\![\Delta]\!] \wedge \eta \in [\![\Delta, \overline{\sigma}]\!] \implies \sigma\eta \in [\![\Delta]\!]$.

Proof. By induction on the depth of the proof of $\eta \in [\![\Delta, \overline{\sigma}]\!]$. □

The following lemma states that proof traces are also closed under interleaving. Differently from Lemma 3.9 above, in this case we cannot use the additional hypotheses $\overline{\sigma}$ when deducing $\eta \in [\![\Delta]\!]$.

Lemma 3.10. $\sigma \in [\![\Delta]\!] \wedge \eta \in [\![\Delta]\!] \implies \sigma \mid \eta \subseteq [\![\Delta]\!]$

Proof. Let Π be a proof of $\sigma \in [\![\Delta]\!]$ (of depth n), and let Ψ be a proof of $\eta \in [\![\Delta]\!]$ (of depth m). The proof proceeds by well-founded induction on the relation $\prec \subseteq \mathbb{N}^2 \times \mathbb{N}^2$ defined as follows:

$$(n', m') \prec (n, m) \iff (n' < n \wedge m' \leq m) \vee (n' \leq n \wedge m' < m)$$

For the base case $(0, 0)$, both Π and Ψ consist only of the axiom (ε), hence the thesis follows trivially. The proof proceeds by considering the last rule used in Π and in Ψ. Full details are in Appendix A. □

The following lemma establishes two basic relations between proof traces and natural deduction proofs in Horn PCL. First, all the atoms in a proof trace of Δ can be deduced from Δ. Second, if some set of atoms is deducible from Δ, then there must exist a proof trace of Δ which contains them all.

Lemma 3.11. *For all Horn* PCL *theories* Δ*:*

(a) $\sigma \in [\![\Delta]\!] \implies \forall a \in \overline{\sigma}.\ \Delta \vdash a$

(b) $\forall a \in \overline{\sigma}.\ \Delta \vdash a \implies \exists \eta \in [\![\Delta]\!].\ \overline{\sigma} \subseteq \overline{\eta}$

A consequence of Lemma 3.11 is that provability in natural deduction can be characterized using proof traces: given a Horn PCL theory Δ, a conjunction of atoms α can be derived from Δ in natural deduction if and only if there exists a proof trace σ of Δ such that all atoms in α belong to σ.

Corollary 3.12. $\Delta \vdash \alpha \iff \exists \sigma \in [\![\Delta]\!].\ \overline{\alpha} \subseteq \overline{\sigma}$

The following lemma is a generalisation of Lemma 3.9 and Lemma 3.10. If $\sigma\nu$ is a proof trace of Δ, we can obtain other proof traces of Δ by appending to σ any interleaving of ν and η, where η is a proof trace η of Δ possibly using $\overline{\sigma}$ as additional hypotheses.

Lemma 3.13. $\sigma\nu \in [\![\Delta]\!] \wedge \eta \in [\![\Delta, \overline{\sigma}]\!] \implies \sigma(\nu \mid \eta) \subseteq [\![\Delta]\!]$

3.4. Urgent atoms

We now define, starting from a Horn PCL theory Δ and a set X of atoms, which atoms may be proved immediately after those in X, following some proof trace. We call these atoms *urgent after* X (in Δ), and we denote then with $\mathcal{U}_\Delta^X$.

Definition 3.14. *For a set* $X \subseteq E$ *and a Horn* PCL *theory* Δ*, we define the set of atoms* $\mathcal{U}_\Delta^X$ *as:*

$$\mathcal{U}_\Delta^X = \{a \notin X \mid \exists \sigma, \sigma'.\ \overline{\sigma} = X \wedge \sigma\, a\, \sigma' \in [\![\Delta, X]\!]\}$$

Example 3.15. *Consider the theory* $\Delta_3 = \{a \to b,\ b \twoheadrightarrow a\}$ *from Example 3.7. We have that:*

- $\mathcal{U}_{\Delta_3}^{\emptyset} = \{a\}$*, because* $a \in [\![\Delta_3]\!] = \{\varepsilon, ab\}$*, and there are no proof traces in* $[\![\Delta_3]\!]$ *starting with* b*.*

- $\mathcal{U}_{\Delta_3}^{\{a\}} = \{b\}$, *because in the proof trace* $ab \in [\![\Delta_3, a]\!] = \{\varepsilon, a, ab\}$, b *is the first atom after those in* $\{a\}$ *(formally, in Definition 3.14 we choose* $\sigma = a$ *and* $\sigma' = \varepsilon$*).*

- $\mathcal{U}_{\Delta_3}^{\{b\}} = \{a\}$, *because in the proof trace* $ba \in [\![\Delta_3, b]\!] = \{\varepsilon, b, ab, ba\}$, *we have that* a *is the first atom after those in* $\{b\}$ *(formally, in Definition 3.14 we choose* $\sigma = b$ *and* $\sigma' = \varepsilon$*).*

- $\mathcal{U}_{\Delta_3}^{\{a,b\}} = \emptyset$, *because there no atoms but* a, b *can occur in the proof traces in* $[\![\Delta_3, a, b]\!]$.

Theorem 3.21 below characterizes urgent atoms in terms of provability. Intuitively, to test if an atom a is urgent after X in Δ, we first decorate with ! the atoms in X (to mean that they have already been proved), and then we encode the clauses in Δ with the mapping $[\cdot]_{\mathcal{U}}$ in Definition 3.16. Then, Theorem 3.21 guarantees that the atom Ua (where the decoration U stands for "urgent") is provable in the Horn PCL theory $[\Delta]_{\mathcal{U}}, !X$ if and only if a is urgent after X.

Technically, Definition 3.16 introduces an endomorphism $[\cdot]_{\mathcal{U}}$ of Horn PCL theories. Let $\star \in \{!, R, U\}$. We assume three injections $\star : E \to E$, such that $!E$, RE and UE are pairwise disjoint. For a set of atoms $X \subseteq E$, we denote with $\star X$ the theory $\{\star e \mid e \in X\}$. Intuitively, the atoms of the form $!a$ correspond to actions already happened in the past, the atoms Ua correspond to urgent actions, while the atoms Ra are those actions which can be eventually reached by performing the urgent ones.

Below, we denote with $atoms(\Delta)$ the set of all atoms in Δ. We assume that $atoms(\Delta) \cap \star E = \emptyset$, and that a stands for an atom not in $\star E$. For a set $X \subseteq !E \cup RE \cup UE$, we define the projection $X^\star = \{e \in E \mid \star e \in X\}$. When $\alpha = a_1 \wedge \cdots \wedge a_n$, we write $\star\alpha$ for the conjunction $\star a_1 \wedge \cdots \wedge \star a_n$. When $n = 0$, $\star\alpha = \top$.

Definition 3.16. *The endomorphism* $[\cdot]_{\mathcal{U}}$ *of Horn* PCL *theories is defined as follows:*

$$
\begin{array}{rcll}
[\Delta, \alpha \triangleright a]_{\mathcal{U}} & = & [\Delta]_{\mathcal{U}} \cup [\alpha \triangleright a]_{\mathcal{U}} \cup \Omega(atoms(\alpha \triangleright a)) & \text{for } \triangleright \in \{\to, \twoheadrightarrow\} \\
\Omega X & = & \{!a \to Ua \mid a \in X\} \cup \{Ua \to Ra \mid a \in X\} & \\
[\alpha \to a]_{\mathcal{U}} & = & \{!\alpha \to Ua,\ R\alpha \to Ra\} & \\
[\alpha \twoheadrightarrow a]_{\mathcal{U}} & = & \{R\alpha \twoheadrightarrow Ua\} &
\end{array}
$$

The ΩX part of the encoding ensures that, intuitively, ! is stronger than U, and that U is stronger than R. In a sense, this is used to assign to each atom a "state" which can be "reachable", "urgent", or "performed". The encoding of an implication $\alpha \to a$ contains $!\alpha \to Ua$, meaning that a becomes urgent when its preconditions α have been done, and $R\alpha \to Ra$, meaning that a is reachable whenever its preconditions are such. The encoding of a contractual implication $\alpha \twoheadrightarrow a$ contains $R\alpha \twoheadrightarrow Ua$, meaning that a is urgent when its preconditions are guaranteed to be reachable.

Example 3.17. *For the* PCL *theory* $\Delta_3 = \{a \to b,\ b \twoheadrightarrow a\}$ *in Example 3.7, we have:*

$$
\begin{array}{rcll}
[\Delta_3]_{\mathcal{U}} & = & \{!a \to Ub,\ \ Ra \to Rb, & (\textit{encoding of } a \to b) \\
 & & \ \ Rb \twoheadrightarrow Ua, & (\textit{encoding of } b \twoheadrightarrow a) \\
 & & \ \ !a \to Ua,\ \ !b \to Ub,\ \ Ua \to Ra,\ \ Ub \to Rb\} & (\Omega\{a, b\})
\end{array}
$$

We have that $[\Delta_3]_{\mathcal{U}} \vdash Ua$ *(see Figure 5 for a proof) and* $[\Delta_3]_{\mathcal{U}} \nvdash Ub$*; also,* $[\Delta_3]_{\mathcal{U}}, !a \vdash Ub$*. Note that our encoding in Definition 3.16 maps contractual implications to contractual implications. This is needed, because if we instead mapped the clause* $b \twoheadrightarrow a$ *to* $Rb \to Ua$ *(i.e. using intuitionistic rather than contractual implication), then no atoms would have been provable in* $[\Delta_3]_{\mathcal{U}}$.

The following lemma is the fundamental technical tool we shall use below to prove our main results about PCL, proof traces, and urgent atoms. It relates the atoms provable in encoded theories $[\Delta]_{\mathcal{U}}$ with the proof traces (item 5a), and with the urgent atoms (item 5b).

$$\dfrac{\dfrac{}{[\Delta_3]_{\mathcal{U}} \vdash Rb \twoheadrightarrow Ua}\,(\text{ID}) \qquad \dfrac{\dfrac{}{[\Delta_3]_{\mathcal{U}}, Ua \vdash Ua \to Ra}\,(\text{ID}) \qquad \dfrac{}{[\Delta_3]_{\mathcal{U}}, Ua \vdash Ua}\,(\text{ID})}{[\Delta_3]_{\mathcal{U}}, Ua \vdash Ra}\,(\to\text{E}) \qquad \dfrac{}{[\Delta_3]_{\mathcal{U}}, Ua \vdash Rb \to Ua}\,(\text{ID})}{[\Delta_3]_{\mathcal{U}}, Ua \vdash Rb}\,(\to\text{E})}{[\Delta_3]_{\mathcal{U}} \vdash Ua}\,(\to\text{E})$$

Figure 5: Natural deduction proof of $[\Delta_3]_{\mathcal{U}} \vdash Ua$.

Lemma 3.18. *For all Horn* PCL *theories* Δ*, for all* $\Gamma \subseteq {!E} \cup UE$*, and for all* α*:*

$$[\Delta]_{\mathcal{U}}, \Gamma \vdash \alpha \implies \begin{cases} \overline{\alpha}^R \subseteq \bigcup \overline{[\![\Delta, \overline{\Gamma}^{!U}]\!]} & \text{(5a)} \\ \overline{\alpha}^U \subseteq \mathcal{U}^{\overline{\Gamma}^!}_{\Delta, \overline{\Gamma}^U} \cup \overline{\Gamma}^{!U} & \text{(5b)} \end{cases}$$

Roughly, item (5a) of Lemma 3.18 states that if one proves in $[\Delta]_{\mathcal{U}}$ some atom of the form Ra, then the atom a belongs to some proof trace of Δ. Similarly, item (5b) states that if Ua is provable in $[\Delta]_{\mathcal{U}}$, then the atom a is urgent in Δ. The proof of Lemma 3.18 is by induction of the derivation of $[\Delta]_{\mathcal{U}} \vdash \alpha$ (see Appendix A for details). Note that the two items only provide one direction of the correspondence between the theories $[\Delta]_{\mathcal{U}}$ and Δ. Lemma 3.19 and Lemma 3.20 refine this result, by also providing the other direction.

The following lemma states that the atoms a for which Ra is derivable from $[\Delta]_{\mathcal{U}}$ are exactly those atoms which occur in some proof trace of Δ.

Lemma 3.19. $a \in \bigcup \overline{[\![\Delta]\!]} \iff [\Delta]_{\mathcal{U}} \vdash Ra$

The following lemma relates proof traces with the *U-atoms*, i.e. the atoms a for which Ua is derivable from $[\Delta]_{\mathcal{U}}$. The ($\Leftarrow$) direction states that (any prefix of) a proof trace is made by U-atoms in sequence. The ($\Rightarrow$) direction states that a finite sequence of U-atoms can be extended to a proof trace.

Lemma 3.20. *Let* $\sigma = \langle e_0 \cdots e_n \rangle$*. Then,*

$$\forall i \in 0..n.\ [\Delta]_{\mathcal{U}}, {!\overline{\sigma_i}} \vdash Ue_i \iff \exists \eta.\ \sigma\eta \in [\![\Delta]\!]$$

The main result about the endomorphism $[\cdot]_{\mathcal{U}}$ follows. Given a Horn PCL theory Δ and a set of atoms X, an atom a is urgent from X in Δ iff Ua is provable in $[\Delta]_{\mathcal{U}}, !X$.

Theorem 3.21. *For all Horn* PCL *theories* Δ*, and for all* $a \notin X \subseteq \mathit{atoms}(\Delta)$*:*

$$a \in \mathcal{U}^X_\Delta \iff [\Delta]_{\mathcal{U}}, !X \vdash Ua$$

Proof. ($\Rightarrow$) Assume that $a \in \mathcal{U}^X_\Delta$. By Definition 3.14, there exist σ, σ' such that $\overline{\sigma} = X$ and $\sigma\, a\, \sigma' \in [\![\Delta, X]\!]$. By Lemma 3.20, we have $[\Delta, X]_{\mathcal{U}}, !X \vdash Ua$. The thesis $[\Delta]_{\mathcal{U}}, !X \vdash Ua$ follows because $[X]_{\mathcal{U}}$ is entailed by $!\top \to UX$, and $!X \to UX$ is obtained by Definition 3.16.

($\Leftarrow$) Assume that $[\Delta]_{\mathcal{U}}, !X \vdash Ua$. Since $[X]_{\mathcal{U}}$ entails $!\top \to UX$, then $[\Delta, X]_{\mathcal{U}} \vdash Ue$ for all $e \in X$. Furthermore, by Lemma 3.8, $[\Delta, X]_{\mathcal{U}}, !X \vdash Ua$. Take any σ such that $\overline{\sigma} = X$. By Lemma 3.20 it follows that there exists some η such that $\sigma\, a\, \eta \in [\![\Delta, X]\!]$. By Definition 3.14, we conclude that $a \in \mathcal{U}^X_\Delta$. □

4. A logical view of contracts

In this section we establish a correspondence between contracts and PCL. In particular, for conflict-free contracts and Horn PCL theories, we shall show that:

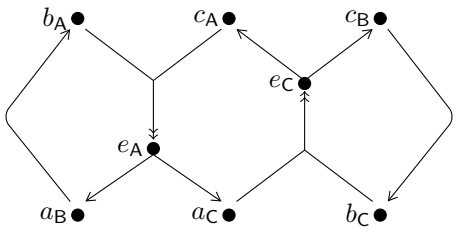

Figure 6: A CES $\mathcal{E}_\star$ for the 3-party escrow scenario.

- agreements can be characterised in terms of provability in PCL (for reachability payoffs, Theorem 4.2);
- sequences of prudent events correspond to (prefixes of) proof traces (Theorem 4.8);
- prudent strategies are those which prescribe to fire urgent atoms in PCL (Theorem 4.11).

For a conflict-free CES $\mathcal{E}$ and a Horn PCL theory Δ, we write $\Delta \sim \mathcal{E}$ when there exists a bijection which maps an enabling $X \vdash e$ in $\mathcal{E}$ to a clause $(\bigwedge X) \to e$ in Δ, and a circular enabling $X \Vdash e$ to $(\bigwedge X) \twoheadrightarrow e$.

Definition 4.1. *We write $\Delta \sim \mathcal{E}$ when $\mathcal{E}$ is finite conflict-free, and*

$$\Delta \;=\; \{(\textstyle\bigwedge X) \to e \mid X \vdash e \in \mathcal{E}\} \cup \{(\textstyle\bigwedge X) \twoheadrightarrow e \mid X \Vdash e \in \mathcal{E}\}$$

To relate agreement with provability, we consider the class of reachability payoffs, which neglect the order in which events are performed (Definition 2.18). This class is quite broad. For instance, it includes the *offer-request payoffs* [24], used by participants which want something in exchange for each provided service.

The following theorem provides us with a logical characterisation of agreements. If Φ is a reachability payoff induced by φ, and $\Delta \sim \mathcal{E}$, then the participant A agrees on the contract $\langle \mathcal{E}, \Phi \rangle$ whenever all the atoms provable in Δ are in the payoff of A.

Theorem 4.2. *Let $\Delta \sim \mathcal{E}$, and let Φ be a reachability payoff induced by φ. Then, A agrees on $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ iff $\{a \mid \Delta \vdash a\} \in \varphi(\mathsf{A})$.*

Example 4.3 (3-party escrow)**.** *Assume three (mutually distrusting) participants want to exchange some items, with the following policy (sketched in Figure 6):*

- A *gives its items to* B *and* C *only after having the acknowledgment from an escrow service* E*;*
- B *gives its item to* A *(resp. to* C*) only after having received the item from* A *(resp. from* C*);*
- C *gives its items to* A *and* B *only after having the acknowledgment from an escrow service* E*;*
- *The escrow service* E *gives the acknowledgment to* A *only under the guarantee that* B *and* C *will eventually give their items to* A*. Similarly for the acknowledgment to* C*.*

We model the participants contracts as follows. Event a_{B} means that A gives an item to B, event b_{C} means that B gives an item to C, etc. Event e_{A} is fired when the escrow service gives its acknowledgment to A (similarly for e_{C}). The obligations are represented by the CES $\mathcal{E}_\star$ *in Figure 6. The composed contract is $\mathcal{C} = \langle \mathcal{E}_\star, \Phi \rangle$, where Φ is the reachability payoff induced by $\varphi = \{E\}$, with $E = \{a_{\mathsf{B}}, a_{\mathsf{C}}, b_{\mathsf{A}}, b_{\mathsf{C}}, c_{\mathsf{A}}, c_{\mathsf{B}}, e_{\mathsf{A}}, e_{\mathsf{C}}\}$.*

The contract $\mathcal{C}$ admits an agreement. To see that, consider the following strategies (explained informally):

- Σ_{A}*: wait e_{A} and then fire a_{B} and a_{C};*
- Σ_{B}*: wait a_{B} and then fire b_{A}; also, wait c_{B} and then fire b_{C};*

- Σ_{C}: *wait* e_{C} *and then fire* c_{A} *and* c_{B}*;*
- Σ_{E}: *fire* e_{A} *and* e_{C}*.*

It is easy to check that all the strategies above are winning in $\mathcal{C}$*. Indeed,* e_{A} *and* e_{C} *are prudent in* ε*;* b_{A} *becomes prudent after* a_{B} *is fired;* b_{C} *after* c_{B}*; events* $a_{\mathsf{B}}, a_{\mathsf{C}}$ *after* e_{A}*; events* $c_{\mathsf{A}}, c_{\mathsf{B}}$ *after* e_{C}*.*

The correspondence between provability in PCL *and agreement in contracts (Theorem 4.2) allows us to transfer this result to* PCL*, by establishing that all the atoms in* E *are provable in the Horn* PCL *theory:*

$$\begin{aligned}\Delta_\star = \{&(b_{\mathsf{A}} \wedge c_{\mathsf{A}}) \twoheadrightarrow e_{\mathsf{A}},\ e_{\mathsf{A}} \to a_{\mathsf{B}},\ e_{\mathsf{A}} \to a_{\mathsf{C}},\ a_{\mathsf{B}} \to b_{\mathsf{A}},\\ &(a_{\mathsf{C}} \wedge b_{\mathsf{C}}) \twoheadrightarrow e_{\mathsf{C}},\ e_{\mathsf{C}} \to c_{\mathsf{A}},\ e_{\mathsf{C}} \to c_{\mathsf{B}},\ c_{\mathsf{B}} \to b_{\mathsf{C}}\}\end{aligned}$$

for which, clearly, $\mathcal{E}_\star \sim \Delta_\star$*. Note that, while of course it is possible to prove that* $\Delta_\star \vdash \bigwedge_{e\in E} e$ *through the proof system of* PCL*, this is not straightforward to see. For instance, it is not obvious that, were any one of the* $\twoheadrightarrow$ *in* $\Delta_\star$ *replaced with a* $\to$*, then no atoms would have been provable.*

To study the relations between contracts and proof traces, it is convenient to first devise an alternative characterisation of prudent events for conflict-free contracts. We denote with $\mathcal{R}^X$ the set *reachable events with past* X. Intuitively, in a set X of past events, we consider an event $e \notin X$ reachable when e occurs in some play $\sigma\eta$ where the prefix σ is a linearization of X, and the credits made in η are honoured. The set $\mathcal{P}^X$ contains the events which can be done in X without eventually augmenting the credits.

Definition 4.4. *For a* CES $\mathcal{E}$ *and a set* $X \subseteq E$*, let:*

$$\begin{aligned}\mathcal{R}^X_{\mathcal{E}} &= \{e \notin X \mid \exists \sigma, \eta :\ \overline{\sigma} = X,\ e \in \overline{\eta},\ \textit{and}\ \Gamma(\sigma\eta) \subseteq X\}\\ \mathcal{P}^X_{\mathcal{E}} &= \{e \notin X \,|\, X \vdash e\ \textit{or}\ X \cup \mathcal{R}^X \Vdash e\}\end{aligned}$$

We omit the index $\mathcal{E}$ *when clear from the context.*

Lemma 4.5. *In finite conflict-free contracts, an event* e *is prudent in* σ *iff* $e \in \mathcal{P}^{\overline{\sigma}}$*.*

The criterion given by Lemma 4.5 is much simpler than the mutually coinductive definition of prudence in Definition 2.12. Indeed, whereas computing prudent events by applying directly Definition 2.12 would give an exponential algorithm, a polynomial-time algorithm for computing $\mathcal{P}^X$ can be obtained as follows. First we compute the set $\mathcal{R}^X$: this can be done by slightly adapting the algorithm described by Theorem 4.8 in [27], which computes the reachable events in a CES. To obtain $\mathcal{R}^X_{\mathcal{E}}$, it suffices to extend the CES $\mathcal{E}$ to $\mathcal{E}' = \mathcal{E} \cup \{\vdash e \mid e \in X\}$, then compute the reachable events of $\mathcal{E}'$ as in [27], and finally remove the events in X. The correctness of this algorithm follows by Lemma 7.60 in [30]. Then, $\mathcal{P}^X$ can be easily computed as in Definition 4.4.

The following example shows that the conflict-free assumption of Lemma 4.5 can not be removed. Indeed, in the presence of conflicts, the set $\mathcal{P}$ can be larger than the set of prudent events.

Example 4.6. *Assume the obligations of two participants* A *and* B *are modelled by the following event structure, where* a *is the event of* A*, and* b_0, b_1 *are those of* B*:*

$$\vdash b_0 \qquad \vdash b_1 \qquad b_0 \Vdash a$$

The event a *is prudent in the empty play, as correctly stated by Lemma 4.5:*

$$\mathcal{R}^\emptyset \;=\; \{a, b_0, b_1\} \;=\; \mathcal{P}^\emptyset$$

However, if we extend the event structure with the conflict $b_0 \# b_1$*, then we still have* $a \in \mathcal{P}^\emptyset$ *(since Definition 4.4 neglects conflicts), while* a *is* not *prudent in the empty play. Indeed, if* B *chooses* b_1*, then he will not have the obligation to do* b_0 *(because of the conflict), hence the credit* a *will not be honoured.*

The following lemma establishes that prudent events in a contract $\langle \mathcal{E}, \cdot \rangle$ correspond to urgent atoms in a PCL theory $\Delta \sim \mathcal{E}$. The idea of the proof is to exploit the endomorphism $[\cdot]_{\mathcal{U}}$ in Definition 3.16 as a bridge between CES and PCL. To do that, we first map $\mathcal{E}$ to the PCL theory $[\Delta]_{\mathcal{U}}$, and we relate the prudent events in $\langle \mathcal{E}, \cdot \rangle$ to the provable atoms in $[\Delta]_{\mathcal{U}}$, which in turn are related to urgent atoms in Δ by Theorem 3.21. Summing up, the prudent events in $\mathcal{E}$ are the urgent atoms in Δ.

Lemma 4.7. *Let $\Delta \sim \mathcal{E}$. Then, for all $X \subseteq E$, $\mathcal{P}^X_{\mathcal{E}} = \mathcal{U}^X_{\Delta}$.*

We can now relate prudence in contracts with proofs in PCL. Theorem 4.8 states that the plays of prudent events correspond to prefixes of proof traces.

Theorem 4.8. *Say $\sigma = \langle e_0 \cdots e_n \rangle$ is a* prudent play *of $\mathcal{E}$ when e_i is prudent for σ_i in $\mathcal{E}$, for all $i \leq n$. If $\Delta \sim \mathcal{E}$, then σ is a prudent play of $\mathcal{E}$ iff $\exists \eta.\ \sigma\eta \in [\![\Delta]\!]$.*

Proof. ($\Rightarrow$) Let $\sigma = \langle e_0 \cdots e_n \rangle$ be a prudent play of $\mathcal{E}$. We proceed by induction on the length of σ. The base case $\sigma = \varepsilon$ is trivial, because $\varepsilon \in [\![\Delta]\!]$ holds by rule (ε). For the inductive case, the induction hypothesis gives that $\sigma_n = \langle e_0 \cdots e_{n-1} \rangle$ is the prefix of a proof trace. By Lemma 3.20, $[\Delta]_{\mathcal{U}}, !\overline{\sigma_i} \vdash U e_i$ for all $i < n$. Since σ is a prudent play, then e_n is prudent in σ_n. By Lemma 4.5, $e_n \in \mathcal{P}^{\overline{\sigma_n}}_{\mathcal{E}}$. By Lemma 4.7, $e_n \in \mathcal{U}^{\overline{\sigma_n}}_{\Delta}$. By Theorem 3.21, $[\Delta]_{\mathcal{U}}, !\overline{\sigma_n} \vdash U e_n$. By Lemma 3.20, there exists η such that $\sigma\eta \in [\![\Delta]\!]$.

($\Leftarrow$) Symmetrical to the other direction. □

Example 4.9. *The prudent plays of the* CES $\mathcal{E}_3$ *in Figure 1 are ε, a, and ab (see Example 2.13). By Theorem 4.8, these can be extended to proof traces in the corresponding Horn* PCL *theory $\Delta_3 \sim \mathcal{E}_3$. Indeed, ab is a proof trace of Δ_3 (see Example 3.7).*

Example 4.10. *Recall the escrow scenario of Example 4.3. The correspondence between contracts and* PCL *allows for easily constructing the proof traces of $\Delta_\star$ — which is not as straightforward by applying directly Definition 3.6. The maximal prudent plays σ are those where only prudent events are fired, i.e.:*

$$\sigma \ \in \ \big(\, e_{\mathsf{A}}\ (a_{\mathsf{C}} \mid a_{\mathsf{B}} b_{\mathsf{A}})\big) \mid \big(\, e_{\mathsf{C}}\ (c_{\mathsf{A}} \mid c_{\mathsf{B}} b_{\mathsf{C}})\big)$$

By Theorem 4.8, these plays exactly correspond to the proof traces of the PCL *theory $\Delta_\star$.*

Our last main result relates the winning strategies of a contract $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ with the proof traces of a PCL theory $\Delta \sim \mathcal{E}$. In particular, for all participants A we construct a strategy that, in a play σ, enables exactly the events of A which are urgent in $\overline{\sigma}$. This strategy is prudent for A, and leads A to a winning play whenever A agrees on $\mathcal{C}$.

Theorem 4.11. *Let $\Delta \sim \mathcal{E}$, and let the strategy Σ_{A} be defined as:*

$$\Sigma_{\mathsf{A}}(\sigma) \ \ = \ \ \mathcal{U}^{\overline{\sigma}}_{\Delta} \ \cap \ \pi^{-1}(\mathsf{A})$$

Then, Σ_{A} is a prudent strategy for A in $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$. Moreover, if Φ is a reachability payoff and $\mathcal{C}$ admits an agreement, then Σ_{A} is winning for A.

Example 4.12 (Shy dancers)**.** *There are n^2 guests at a wedding party, arranged in a grid of size $n \times n$. The music starts, the guests would like to dance, but they are too timid to start. Each guest will dance provided that at least other two guests in its 8-cells neighborhood will do the same.*

We model this scenario as follows. For all $i, j \in 1..n$, $\mathsf{A}_{i,j}$ is the guest at cell (i, j), and $e_{i,j}$ is the event which models $\mathsf{A}_{i,j}$ dancing. The neighborhood of (i, j) is $I_{i,j} = \{(p, q) \neq (i, j) \mid |p - i| \leq 1 \ \wedge \ |q - j| \leq 1\}$, and we define $E_{i,j} = \{e_{p,q} \mid (p, q) \in I_{i,j}\}$.

Let $\mathfrak{F}$ be the set of functions from $\{1..n\} \times \{1..n\}$ to $\{\vdash, \Vdash\}$. Intuitively, each function $\bullet \in \mathfrak{F}$ establishes which guests use $\vdash$ and which use $\Vdash$. For all $\bullet \in \mathfrak{F}$ and for all $i, j \in 1..n$, guest $\mathsf{A}_{i,j}$ promises to dance if at least two neighbours have already started (in case $\bullet(i, j) = \vdash$), or under the guarantee that they will eventually dance (when $\bullet(i, j) = \Vdash$). Formally, for all $\bullet \in \mathfrak{F}$, let $\mathcal{E}^\bullet$ be the CES*:*

$$\mathcal{E}^\bullet \ = \ \bigcup_{i,j \in 1..n} \mathcal{E}^\bullet_{i,j} \qquad \text{where} \ \ \mathcal{E}^\bullet_{i,j} \ = \ \{X \bullet (i, j)\ e_{i,j} \mid X \subseteq E_{i,j} \ \wedge \ |X| = 2\}$$

The objective of a participant $\mathsf{A}_{i,j}$ is to reach a play where at least two participants in its neighborhood $E_{i,j}$ are dancing. This is modelled by the function Φ such that $\Phi(\mathsf{A}_{i,j}) = \{\sigma \mid \overline{\sigma} \cap E_{i,j} \geq 2\}$, for all $i, j \in 1..n$. For all $\bullet \in \mathfrak{F}$, we ask whether the contract $\mathcal{C}^\bullet = \langle \mathcal{E}^\bullet, \Phi \rangle$ admits an agreement, i.e. if all guests will eventually dance. We can prove that $\mathcal{C}^\bullet$ admits an agreement iff there exist two guests in the same neighborhood which use $\Vdash$. Formally:

$$\exists i, j \in 1..n.\ \exists (p,q), (p',q') \in I_{i,j}.\ (p,q) \neq (p',q')\ \wedge\ \bullet(p,q) = \Vdash = \bullet(p',q')$$

Indeed, when the above holds, the strategy:

$$\Sigma^\bullet_{i,j}(\sigma)\ =\ \begin{cases} \{e_{i,j}\} & \text{if } e_{i,j} \notin \overline{\sigma}, \text{ and } \bullet(i,j) = \Vdash \text{ or } \overline{\sigma} \vdash e_{i,j} \\ \emptyset & \text{otherwise} \end{cases}$$

is winning, for all guests $\mathsf{A}_{i,j}$. As noted in the previous example, the correspondence established by Theorem 4.2 allows us to transfer the above observations to PCL. *In particular, the above provides a simple proof that, in the Horn* PCL *theory:*

$$\Delta^\bullet\ =\ \{\alpha \bullet (i,j)\ e_{i,j} \mid \overline{\alpha} \subseteq E_{i,j}\ \wedge\ |\overline{\alpha}| \geq 2\ \wedge\ i, j \in 1..n\}$$

some atom is provable iff there exist at least two distinct clauses which use $\twoheadrightarrow$. Again, this result would not be easy to prove directly, without exploiting the correspondence between agreements and provability.

5. Related work and Conclusions

We have studied the relations between a foundational models for contracts and the logic PCL. The main result is that the notions of agreement, prudent plays and winning strategies in the game-theoretic model of [24] have been related, respectively, to that of provability, proof traces and urgent atoms in the logical model of [15] (Theorem 4.2, Theorem 4.8, and Theorem 4.11).

The motivations underlying PCL and CES are related to those introduced in [14] to compose assume-guarantee specifications [31]. Circularity in assume-guarantee reasoning is created whenever a system will give some guarantee M_1 about its behaviour, provided that the environment it operates within will behave according to some assumption M_2, and *vice versa*. In the model of [14], circular reasoning is represented by the judgment $(M_1 \to M_2) \wedge (M_2 \to M_1) \vdash M_1 \wedge M_2$. However, since $\to$ is the usual intuitionistic implication, such judgment is not generally valid (as in IPC) but is subject to a side condition on the interpretation of M_1, M_2 in the model. In PCL, instead, circularity is handled using a specific implication connective $\twoheadrightarrow$, whose axiomatization does not affect the IPC fragment of PCL — PCL being a conservative extension of IPC. A similar idea was followed in CES: instead of trying to suitably change the role of the enabling relation $\vdash$ to address circularity, a new relation $\Vdash$ is added to such purpose. Further, unlike [14], PCL reasoning is not tailored upon any specific model. Still, we were able to relate CES and PCL, making it possible to think about CES as a model of the Horn fragment of PCL. Actually, finding a class of models on which general circular reasoning is sound and complete appears to be hard: e.g. [32] shows the impossibility of devising, in some lattice-based models, a sound and complete set of compositional rules for circular assume-guarantee.

The contract model used in this paper has been borrowed from [24]. Besides agreement, the other crucial notion introduced in [24] is that of *protection*: intuitively, a participant is protected by a contract when she has a strategy to defend herself in all possible contexts, even in those where she has not reached an agreement. A first result of [24] is that, using standard ES (without circular causality), agreements and protection mutually exclude each other. Then, it is shown that circular enablings allow for constructing contracts which guarantee both agreements and protection. While [24] is not concerned with relating contracts with PCL, putting together these results with the correspondences obtained in this paper may give insights about the computational meaning of the contractual implication connective of PCL.

Some preliminary work on relating event structures with the logic PCL has been reported in [5]. The model of [5] is a simplified version of that considered in the current paper: it does not exploit game-theoretic

notions, conflicts are not considered, events are finite, payoffs are just sets of events, and agreement is defined as the existence of a configuration in the CES which contains such set. In this simple model, it is shown that an event is reachable in a CES whenever it is provable in the corresponding PCL theory. Hence, an agreement exists whenever all the events in the payoff of each participant are provable. Theorem 4.2 extends this result to a more general (game-theoretic) notion of agreement and of payoff.

Event structures with circular causality are thoroughly investigated in [27]. There, CES are considered in their full generality: they allow for infinite sets of events, and can model non-determinism through the conflict relation. A relation between CES and PCL is then established: roughly, the problem of deciding if some set of events is a configuration of a CES is reduced to that of proving a certain formula in PCL. Also, [27] introduces the notion of urgent events, i.e. those events which always allow to eventually reach a state with empty credits. While [27] does not feature a correspondence between urgent events and PCL, this is provided by Theorem 3.21 in this paper, which relates urgent events to provability in PCL. Note that the definition of urgent events in [27] implicitly assumes that non-deterministic choices are angelic, so representing a situation where participants *cooperate* to reach a common goal. To model participants which *compete* to reach their individual goals requires instead the game-theoretic machinery (demonic choices, strategies, innocence, prudence, winning plays, *etc.*) introduced in [24].

An encoding of Horn PCL formulae into a variant of CCS has been presented in [33]. Very roughly, the encoding maps a clause $\alpha \to a$ in a process which inputs all the channels in α and then outputs on a, while a clause $\alpha \twoheadrightarrow a$ the input of α and the output of a is done in parallel. The actual encoding is more sophisticated than the above intuition, mostly because it has to take into account multiple participants which share the same channels, and it has to agree with the notion of culpability defined in the logical model. In particular, in the CCS model a participant is considered culpable only when omitting to produce a promised output, or omitting to input an available message. The correspondence result (Theorem 2.7 in [33]) states that provable atoms in PCL are exactly those atoms that are communicated by participants in those CCS traces which lead to a state in which each no culpable participant is present.

In [34] an extension of linear logic, called *cancellative linear logic*, is defined, out of an analysis of some categorical models of linear logic, where the $\otimes$ and $\parr$ operators are identified. As a consequence, linear implication $a \multimap b$ can be used in two ways: either one feeds it with the resource a to get the resource b, or one gets the resource b while introducing at the same time a *debt* $a^{\perp}$, which can be settled later in the presence of an occurence of the resource a. Cancellative linear logic presents some similarities with PCL, as both approaches allow to logically represent obligations. The main difference between these logics is the way debts are dealt with: while in cancellative linear logic debts can be used without restraints, in PCL obligations are introduced in a controlled way, guaranteeing that all debts will eventually be settled.

In [3] the idea of performing events "on credit" has been explored in the domain of Petri nets. In the variant of Petri nets presented in [3] (called Lending Petri nets, LPNs), certain places may be tagged as "lending", with the meaning that their marking can become negative, but must be eventually brought back to a nonnegative value (i.e. the marking is "honoured"). A technique is presented to transform Horn PCL theories into LPNs, and it is shown that provability in a PCL theory corresponds to *weak termination* in the LPN obtained by the transformation. A similar approach is that of *financial games* in Petri nets [34], where moves allow for creating *debts*, and for annihilating debts with credits. A difference between LPNs and financial games is that in the latter debits (modelled as negative tokens) can be always created, whereas in LPNs they can only be created by lending places. Also, the annihilation of positive and negative tokens in financial games is not present in LPNs, which instead use honoured markings to detect successful computations. Models of contracts based on Petri nets, like those mentioned above, seem less expressive than the contracts considered of this paper, as they implicitly assume that non-deterministic choices are angelic, so representing a situation where participants *cooperate* to reach a common goal. Modelling the more general case where participants may *compete* to reach their goals requires the game-theoretic machinery used here.

Studying contracts and circular causality in a resource-aware logic is a future object of study of ours. In particular, it seems that there is connection between intuitionistic linear logic with mix [35] and Petri Nets with debit arcs [36], similarly to the connection between PCL and CES-based contracts studied in this paper. Establishing such correspondence could lead to algorithms for provability in (the Horn fragment of) the logic, exploiting the decision procedures on Petri nets.

References

[1] OASIS, Reference architecture foundation for service oriented architecture, comm. Spec. 01, v.1.0. Available at http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.html (December 2012).

[2] W. M. P. van der Aalst, N. Lohmann, P. Massuthe, C. Stahl, K. Wolf, Multiparty contracts: Agreeing and implementing interorganizational processes, Comput. J. 53 (1) (2010) 90–106. doi:10.1093/comjnl/bxn064.

[3] M. Bartoletti, T. Cimoli, G. M. Pinna, Lending Petri nets and contracts, in: Proc. FSEN, Vol. 8161 of LNCS, Springer, 2013, pp. 66–82. doi:10.1007/978-3-642-40213-5_5.

[4] T. T. Hildebrandt, R. R. Mukkamala, Declarative event-based workflow as distributed dynamic condition response graphs, in: Proc. PLACES, Vol. 69 of EPTCS, 2010, pp. 59–73. doi:10.4204/EPTCS.69.5.

[5] M. Bartoletti, T. Cimoli, G. M. Pinna, R. Zunino, An event-based model for contracts, in: Proc. PLACES, Vol. 109 of EPTCS, 2012, pp. 13–20. doi:10.4204/EPTCS.109.3.

[6] L. Bocchi, K. Honda, E. Tuosto, N. Yoshida, A theory of design-by-contract for distributed multiparty interactions, in: Proc. CONCUR, Vol. 6269 of LNCS, 2010, pp. 162–176. doi:10.1007/978-3-642-15375-4_12.

[7] M. Bravetti, I. Lanese, G. Zavattaro, Contract-driven implementation of choreographies, in: Proc. TGC, Vol. 5474 of LNCS, 2008, pp. 1–18. doi:10.1007/978-3-642-00945-7_1.

[8] M. Bravetti, G. Zavattaro, Contract based multi-party service composition, in: Proc. FSEN, Vol. 4767 of LNCS, 2007, pp. 207–222. doi:10.1007/978-3-540-75698-9_14.

[9] G. Castagna, N. Gesbert, L. Padovani, A theory of contracts for web services, ACM TOPLAS 31 (5) (2009) 19:1–19:61. doi:10.1145/1538917.1538920.

[10] K. Honda, N. Yoshida, M. Carbone, Multiparty asynchronous session types, in: Proc. POPL, 2008, pp. 273–284. doi:10.1145/1328438.1328472.

[11] A. Lomuscio, W. Penczek, M. Solanki, M. Szreter, Runtime monitoring of contract regulated web services, Fundamenta Informaticae 111 (3) (2011) 339–355. doi:10.3233/FI-2011-566.

[12] F. Raimondi, J. Skene, W. Emmerich, Efficient online monitoring of web-service SLAs, in: SIGSOFT FSE, 2008, pp. 170–180. doi:10.1145/1453101.1453125.

[13] M. Abadi, M. Burrows, B. Lampson, G. Plotkin, A calculus for access control in distributed systems, ACM TOPLAS 4 (15) (1993) 706–734. doi:10.1145/155183.155225.

[14] M. Abadi, G. D. Plotkin, A logical view of composition, Theoretical Computer Science 114 (1) (1993) 3–30. doi:10.1016/0304-3975(93)90151-I.

[15] M. Bartoletti, R. Zunino, A calculus of contracting processes, in: Proc. LICS, 2010, pp. 332–341. doi:10.1109/LICS.2010.25.

[16] C. Prisacariu, G. Schneider, A dynamic deontic logic for complex contracts, The Journal of Logic and Algebraic Programming (JLAP) 81 (4) (2012) 458–490. doi:10.1016/j.jlap.2012.03.003.

[17] J. Gelati, A. Rotolo, G. Sartor, G. Governatori, Normative autonomy and normative co-ordination: Declarative power, representation, and mandate, Artificial Intelligence and Law 12 (1-2) (2004) 53–81. doi:10.1007/s10506-004-1922-2.

[18] K. Honda, A. Mukhamedov, G. Brown, T.-C. Chen, N. Yoshida, Scribbling interactions with a formal foundation, in: Distributed Computing and Internet Technology, 2011, pp. 55–75. doi:10.1007/978-3-642-19056-8_4.

[19] K. Honda, Types for dyadic interaction, in: CONCUR, 1993, pp. 509–523.

[20] K. Honda, V. T. Vasconcelos, M. Kubo, Language primitives and type disciplines for structured communication-based programming, in: Proc. ESOP, 1998. doi:10.1007/BFb0053567.

[21] T.-C. Chen, L. Bocchi, P.-M. Deniélou, K. Honda, N. Yoshida, Asynchronous distributed monitoring for multiparty session enforcement, in: Proc. TGC, 2011, pp. 25–45.

[22] M. Armbrust, et al., A view of cloud computing, Comm. ACM 53 (4) (2010) 50–58. doi:10.1145/1721654.1721672.

[23] H. Haas, Designing the architecture for web services — W3C (2003).

[24] M. Bartoletti, T. Cimoli, R. Zunino, A theory of agreements and protection, in: Proc. POST, Vol. 7796 of LNCS, Springer, 2013, pp. 186–205. doi:10.1007/978-3-642-36830-1_10.

[25] G. Winskel, Event structures, in: Advances in Petri Nets, 1986, pp. 325–392. doi:10.1007/3-540-17906-2_31.

[26] S. Abramsky, P.-A. Mellies, Concurrent games and full completeness, in: Proc. LICS, 1999, pp. 431–431.

[27] M. Bartoletti, T. Cimoli, G. M. Pinna, R. Zunino, Circular causality in event structures, Fundamenta Informaticae 134 (3-4). doi:10.3233/FI-2014-1101.

[28] S. Kleene, Introduction to metamathematics, North-Holland Publishing Company, 1952.

[29] J.-Y. Girard, P. Taylor, Y. Lafont, Proofs and types, Cambridge University Press, New York, NY, USA, 1989.

[30] T. Cimoli, A theory of agreements and protection, Ph.D. thesis, University of Cagliari (2013).

[31] M. Abadi, L. Lamport, Composing specifications, ACM Transactions on Programming Languages and Systems 15 (1) (1993) 73–132.

[32] P. Maier, Compositional circular assume-guarantee rules cannot be sound and complete, in: FoSSaCS, Vol. 2620 of Lecture Notes in Computer Science, Springer, 2003, pp. 343–357.

[33] M. Bartoletti, E. Tuosto, R. Zunino, Contract-oriented computing in CO_2, Scientific Annals in Computer Science 22 (1) (2012) 5–60. doi:10.7561/SACS.2012.1.5.

[34] N. Martí-Oliet, J. Meseguer, From Petri nets to linear logic, Mathematical Structures in Computer Science 1 (1) (1991) 69–101.

[35] A. Fleury, C. Retoré, The mix rule, Mathematical Structures in Computer Science 4 (2) (1994) 273–285.

[36] P. D. Stotts, P. Godfrey, Place/transition nets with debit arcs, Inf. Process. Lett. 41 (1) (1992) 25–33. doi:10.1016/0020-0190(92)90076-8.

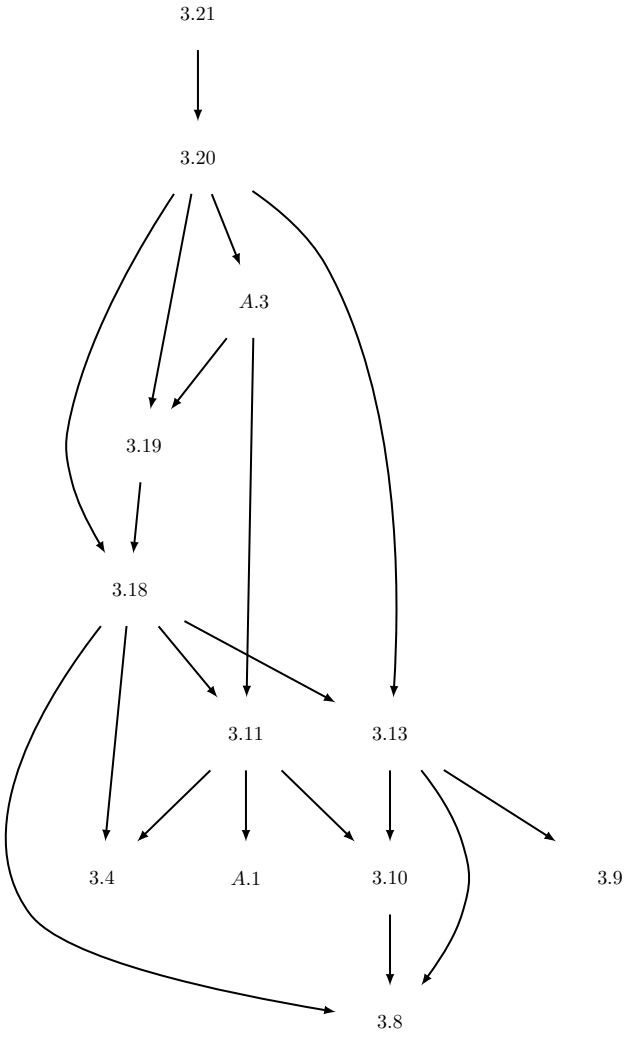

Figure 7: Dependencies among the proofs.

A. Proofs for Section 3

The diagram in Figure 7 illustrates the dependencies among the proofs.

Lemma A.1 (Cut)**.** *In the natural deduction system for* PCL*, if* $\Delta \vdash p$ *and* $\Delta, p \vdash q$ *then* $\Delta \vdash q$*.*

Proof. We have the following proof in the natural deduction system of PCL:

$$\dfrac{\dfrac{\Delta, p \vdash q}{\Delta \vdash p \to q}\,(\to\mathrm{I}) \qquad \Delta \vdash p}{\Delta \vdash q}\,(\to\mathrm{E})$$

□

Theorem 3.2. $\Delta \vdash p$ *is provable in natural deduction iff* $\Delta \vdash p$ *is provable in the sequent calculus of [15].*

Proof. For the "if" part, assume that there exists a sequent calculus proof $\tilde{\pi}$ of $\Delta \vdash r$. We proceed by induction on the height of $\tilde{\pi}$. We only have to consider the cases when the last rule of $\tilde{\pi}$ uses a $\twoheadrightarrow$ formula,

$$\frac{}{\Delta, p \vdash p}\ (\textsc{Id}) \qquad \frac{\Delta \vdash p \quad \Delta,\ p \vdash q}{\Delta \vdash q}\ (\textsc{Cut}) \qquad \frac{\Delta,\ p \to q \vdash p \quad \Delta,\ p \to q,\ q \vdash r}{\Delta,\ p \to q \vdash r}\ (\to\text{L}) \qquad \frac{\Delta,\ p \vdash q}{\Delta \vdash p \to q}\ (\to\text{R})$$

$$\frac{\Delta \vdash q}{\Delta \vdash p \twoheadrightarrow q}\ (\textsc{Zero}) \qquad \frac{\Delta,\ p \twoheadrightarrow q,\ p' \vdash p \quad \Delta,\ p \twoheadrightarrow q,\ q \vdash p' \twoheadrightarrow q'}{\Delta,\ p \twoheadrightarrow q \vdash p' \twoheadrightarrow q'}\ (\textsc{Lax}) \qquad \frac{\Delta,\ p \twoheadrightarrow q,\ r \vdash p \quad \Delta,\ p \twoheadrightarrow q,\ q \vdash r}{\Delta,\ p \twoheadrightarrow q \vdash r}\ (\textsc{Fix})$$

$$\frac{\Delta,\ p \wedge q,\ p \vdash r}{\Delta,\ p \wedge q \vdash r}\ (\wedge\text{L1}) \qquad \frac{\Delta,\ p \wedge q,\ q \vdash r}{\Delta,\ p \wedge q \vdash r}\ (\wedge\text{L2}) \qquad \frac{\Delta \vdash p \quad \Delta \vdash q}{\Delta \vdash p \wedge q}\ (\wedge\text{R})$$

$$\frac{\Delta, p \vee q, p \vdash r \quad \Delta, p \vee q, q \vdash r}{\Delta, p \vee q \vdash r}\ (\vee\text{L}) \qquad \frac{\Delta \vdash p}{\Delta \vdash p \vee q}\ (\vee\text{R1}) \qquad \frac{\Delta \vdash q}{\Delta \vdash p \vee q}\ (\vee\text{R2})$$

$$\frac{\Delta, \neg p \vdash p}{\Delta, \neg p \vdash r}\ (\neg\text{L}) \qquad \frac{\Delta, p \vdash \bot}{\Delta \vdash \neg p}\ (\neg\text{R}) \qquad \frac{}{\Delta, \bot \vdash p}\ (\bot\text{L}) \qquad \frac{}{\Delta \vdash \top}\ (\top\text{R}) \qquad \frac{\Delta \vdash \bot}{\Delta \vdash p}\ (\textsc{WeakR})$$

Figure 8: Genzten-style proof system for PCL.

since all other cases follows from the equivalence between provability in sequent calculus and provability in natural deduction for intuitionistic logic [29].

- (Zero). Straightforward from the induction hypothesis, by applying the ($\to$I1) introduction rule of natural deduction.
- (Lax). We have $\Delta = \Delta', p \twoheadrightarrow q$, $r = p' \twoheadrightarrow q'$, and:

  $$\frac{\Delta,\ p' \vdash p \qquad \Delta,\ q \vdash r}{\Delta \vdash r}\ (\textsc{Lax})$$

  By applying the induction hypothesis on both premises, we obtain two natural deduction proofs π_1, π_2 of $\Delta, p' \vdash p$ and $\Delta, q \vdash r$, respectively. Let π_3 be a natural deduction proof of $\Delta \vdash p \twoheadrightarrow q$, obtained by rule (Id). We combine π_1, π_2 and π_3 by applying rule ($\twoheadrightarrow$I2), from which we obtain a natural deduction proof of $\Delta \vdash r$.
- (Fix). We have $\Delta = \Delta', p \twoheadrightarrow q$, and:

  $$\frac{\Delta,\ r \vdash p \quad \Delta,\ q \vdash r}{\Delta \vdash r}$$

  By applying the induction hypothesis on both premises, we obtain two natural deduction proofs π_1, π_2 of $\Delta, r \vdash p$ and of $\Delta, q \vdash r$, respectively. By Lemma A.1, there exists a natural deduction proof π_3 of $\Delta, q \vdash p$. Let π_4 be a natural deduction proof of $\Delta \vdash p \twoheadrightarrow q$, obtained by rule (Id). We then construct the following natural deduction proof:

  $$\dfrac{\dfrac{\Delta, q \vdash r}{\Delta \vdash q \to r}\ (\to\text{I}) \qquad \dfrac{\dfrac{}{\Delta \vdash p \twoheadrightarrow q}\ (\textsc{Id}) \qquad \Delta, q \vdash p}{\Delta \vdash q}\ (\twoheadrightarrow\text{E})}{\Delta \vdash r}\ (\to\text{E})$$

For the "only if" part, we proceed by induction on the height of the natural deduction proof π of $\Delta \vdash a$. As before, we only consider the cases concerning $\twoheadrightarrow$ formulas.

1. if π ends with a ($\to$I1) rule it is straightforward from induction hypothesis applying the (Zero) rule of sequent calculus.

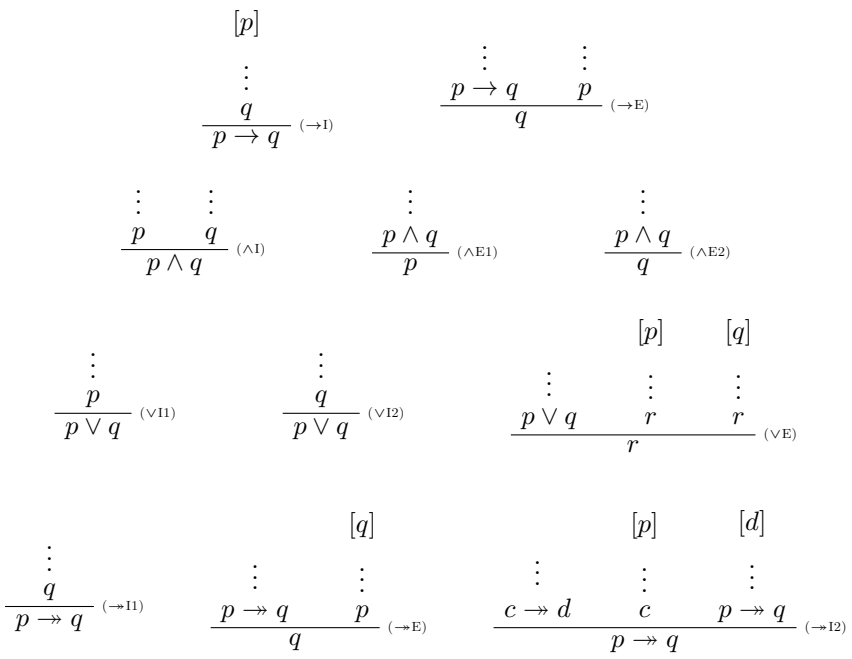

Figure 9: Natural deduction tree-style rules for PCL.

2. if π ends with an ($\twoheadrightarrow$E) rule, then by induction hypothesis on the proofs π_1, π_2 premises of π we get two sequent calculus proofs π_1^* of $\Delta \vdash p \twoheadrightarrow q$ and π_2^* of $\Delta, q \vdash p$. By structural properties, we can change π_2^* with $\pi_2^{'*}$ with conclusions $\Delta, p \twoheadrightarrow q, q \vdash p$. From $\pi_2^{'*}$ and $\Delta, p \twoheadrightarrow q, q \vdash q$ we obtain a proof of $\Delta, p \twoheadrightarrow q \vdash q$ using a (Fix) rule; by composing it with π_1^* using a cut rule we get a sequent calculus proof of $\Delta \vdash q$.

3. if π ends with ($\twoheadrightarrow$I2), then by induction hypothesis on the proofs π_1, π_2, π_3 premises of π we get the sequent calculus proofs π_1^* of $\Delta \vdash p \twoheadrightarrow q$, π_2^* of $\Delta, a \vdash p$ and a proof π_3^* of $\Delta, q \vdash c \twoheadrightarrow d$.

   By structural properties, we can change π_2^* with $\pi_2^{'*}$ with conclusions $\Delta, p \twoheadrightarrow q, c \vdash p$ (resp. π_3^* with $\pi_3^{'*}$ with conclusions $\Delta, p \twoheadrightarrow q, q \vdash c \twoheadrightarrow d$).

   From $\pi_2^{'*}$ and $\pi_3^{'*}$ we obtain a proof of $\Delta, p \twoheadrightarrow q \vdash c \twoheadrightarrow d$ using a (Lax); by composing it using a cut rule with π_1^* we get a sequent calculus proof of $\Delta \vdash c \twoheadrightarrow d$.

□

In the proof of the following lemma it is convenient to use an alternative (equivalent) presentation of natural deduction proofs for PCL, called *tree-like*. In this presentation a proof of a formula p from a set of formulae Δ is a tree having root p and as leaves elements of Δ. The tree is built following the rules in Figure 9. We recall that bracketed formulas are called *discharged*, and do not count as leaves.

We will call the presentation of natural deduction proofs provided in the main text *sequent-like*, to distinguish it from the tree-like one.

Lemma A.2. *Let π be a* PCL *tree-style natural deduction proof of p with assumption Δ, which uses only the rules* ($\wedge$I), ($\wedge$E1), ($\wedge$E2), ($\rightarrow$E), *and* ($\twoheadrightarrow$E)*; then there exists a* PCL *sequent-like natural deduction proof π' of $\Delta \vdash p$ which uses only the rules* (Id), ($\wedge$I), ($\wedge$E1), ($\wedge$E2), ($\rightarrow$E), *and* ($\twoheadrightarrow$E).

Proof. Straightforward verification, by induction on the height of π. □

Lemma 3.4. *Let Δ be a Horn* PCL *theory. If $\Delta \vdash \alpha$ in natural deduction, then a proof of $\Delta \vdash \alpha$ exists which uses only the rules* (Id), ($\wedge$I), ($\wedge$E1), ($\wedge$E2), ($\rightarrow$E), *and* ($\twoheadrightarrow$E).

Proof. Let us take a natural deduction proof π of $\Delta \vdash \alpha$. By Theorem 3.2, there exists a proof $\tilde{\pi}$ of $\Delta \vdash \alpha$ in sequent calculus. Since PCL enjoys cut elimination and the subformula property [15], there exists a proof $\tilde{\pi}'$ of $\Delta \vdash \alpha$ in sequent calculus which uses only the rules ($\to$L), (Fix), ($\wedge$L1), ($\wedge$L2), ($\wedge$R) and (Id). We construct by induction on the heigth of $\tilde{\pi}'$ a tree-like natural deduction proof π' of α from Δ only using the rules ($\wedge$I), ($\wedge$E1), ($\wedge$E2), ($\to$E), and ($\twoheadrightarrow$E). We have the following exhaustive cases, according to the last rule used in $\tilde{\pi}'$:

- (Id). Then, π' is a tree-style natural deduction proof consisting just of the leaf α, included in the set of formulae $\Delta \cup \{\alpha\}$.
- ($\to$L). We have that $\Delta = \Delta', \beta \to b$, and:

$$\frac{\Delta \vdash \beta \qquad \Delta, b \vdash \alpha}{\Delta \vdash \alpha}$$

  Let $\tilde{\pi}'_1$ and $\tilde{\pi}'_2$ be the proofs used in the first and in the second premise, respectively. By applying the induction hypothesis twice, we obtain a natural deduction proof π'_1 of β from Δ, and a natural deduction proof π'_2 of α from $\Delta \cup \{b\}$. From π'_1 and $\beta \to b$, by rule ($\to$E) we obtain a proof π'_3 of b from $\Delta \cup \{\beta \to b\}$; then we replace in π'_2 the leaf corresponding to b with the proof π'_3 to get a proof π' of α from $\Delta \cup \{\beta \to b\}$. If such a leaf does not exists in π'_2 we simply take π'_2 as π', replacing the set $\Delta \cup \{b\}$ with $\Delta \cup \{\beta \to b\}$.
- (Fix). We have that $\Delta = \Delta', \beta \twoheadrightarrow b$, and:

$$\frac{\Delta, \alpha \vdash \beta \qquad \Delta, b \vdash \alpha}{\Delta \vdash \alpha}$$

  Let $\tilde{\pi}'_1$ and $\tilde{\pi}'_2$ be the proofs used in the first and in the second premise, respectively. By applying the induction hypothesis twice, we obtain a natural deduction proof π'_1 of β from $\Delta \cup \{\alpha\}$, and a natural deduction proof π'_2 of α from $\Delta \cup \{b\}$.

  By replacing in π'_1 the leaf corresponding to α with the proof π'_2 we get a proof π'_3 of β from $\Delta \cup \{b\}$ (if there is not a leaf corresponding to α in π'_1 we simply take π'_2 as π'_3).

  From π'_3 and $\beta \twoheadrightarrow b$ by a ($\twoheadrightarrow$E) rule we get a proof π'_4 of b from Δ; then we replace in π'_2 the leaf corresponding to b with the proof π'_4 to get a proof π' of α from Δ (if there is not a leaf corresponding to $\{b\}$ in π'_2 we simply take π'_2 as π', replacing the set $\Delta \cup \{b\}$ with Δ).
- ($\wedge$L1). We have that $\Delta = \Delta', \beta_1 \wedge \beta_2$, and:

$$\frac{\Delta, \beta_1 \vdash \alpha}{\Delta \vdash \alpha}$$

  By induction on the proof $\tilde{\pi}'_1$ of the premise, we get a natural deduction proof π'_1 of α from $\Delta \cup \{\beta_1\}$. Consider the proof π'_2 of β_1 from $\beta_1 \wedge \beta_2$ obtained by taking $\beta_1 \wedge \beta_2$ as hypothesis and applying rule ($\wedge$E1). If we replace in π'_1 the leaf corresponding to β_1 with the proof π'_2 we get a proof π' of α from $\Delta = \Delta' \cup \{\beta_1 \wedge \beta_2\}$. If such a leaf does not exists in π'_1 we simply take π'_1 as π', replacing the set $\Delta \cup \{\beta_1\}$ with $\Delta = \Delta' \cup \{\beta_1 \wedge \beta_2\}$.
- ($\wedge$L2). Symmetrical to the previous case.
- ($\wedge$R). Straightforward by the induction hypothesis and by rule ($\wedge$I).

We obtain in this way a tree-like natural deduction proof π', which uses only the rules ($\wedge$I), ($\wedge$E1), ($\wedge$E2), ($\to$E), and ($\twoheadrightarrow$E). By applying Lemma A.2, we get a proof π in sequent-like natural deduction which uses only the rules (Id), ($\wedge$I), ($\wedge$E1), ($\wedge$E2), ($\to$E), and ($\twoheadrightarrow$E). □

Lemma 3.10. $\sigma \in [\![\Delta]\!] \ \wedge \ \eta \in [\![\Delta]\!] \implies \sigma \mid \eta \subseteq [\![\Delta]\!]$

Proof. We will prove the lemma by well-founded induction on the relation $\prec \subseteq \mathbb{N}^2 \times \mathbb{N}^2$ defined as follows:

$$(n', m') \prec (n, m) \iff (n' < n \ \wedge \ m' \leq m) \ \vee \ (n' \leq n \ \wedge \ m' < m)$$

Let Π be a proof of $\sigma \in [\![\Delta]\!]$ (of depth n), and let Ψ be a proof of $\eta \in [\![\Delta]\!]$ (of depth m).

For the base case $(0, 0)$, both Π and Ψ consist only of the axiom (ε), hence the thesis follows trivially, because $\varepsilon \mid \varepsilon = \{\varepsilon\}$.

For the inductive cases, we have the following subcases, according to the last rule used in Π and in Ψ (symmetric cases are omitted)

- $(\varepsilon)/-$. We have that $\sigma = \varepsilon$. The thesis follows because $\sigma \mid \eta = \varepsilon \mid \eta = \{\eta\} \subseteq [\![\Delta]\!]$.
- $(\to)/(\to)$. For some σ', η', a, b, such that $\sigma = \sigma' a$ and $\eta = \eta' b$, we have:

$$\frac{\alpha \to a \in \Delta \qquad \sigma' \in [\![\Delta]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma'}}{\sigma' \, a \in [\![\Delta]\!]} \qquad \frac{\beta \to b \in \Delta \qquad \eta' \in [\![\Delta]\!] \qquad \overline{\beta} \subseteq \overline{\eta'}}{\eta' \, b \in [\![\Delta]\!]}$$

  We now apply the induction hypothesis twice: by the premise $\sigma' \in [\![\Delta]\!]$, we obtain $\sigma' \mid \eta \subseteq [\![\Delta]\!]$; by the premise $\eta' \in [\![\Delta]\!]$, we obtain $\sigma \mid \eta' \subseteq [\![\Delta]\!]$. By the rule $(\to)$, we have:

$$\begin{aligned} \alpha \to a \in \Delta, \quad \sigma' \mid \eta \subseteq [\![\Delta]\!], \quad (\forall \tau \in \sigma' \mid \eta. \ \overline{\alpha} \subseteq \overline{\tau}) \implies (\sigma' \mid \eta) \, a \subseteq [\![\Delta]\!] \\ \beta \to b \in \Delta, \quad \sigma \mid \eta' \subseteq [\![\Delta]\!], \quad (\forall \tau \in \sigma \mid \eta'. \ \overline{\beta} \subseteq \overline{\tau}) \implies (\sigma \mid \eta') \, b \subseteq [\![\Delta]\!] \end{aligned}$$

  The thesis follows because $\sigma \mid \eta = (\sigma' a) \mid (\eta' b) = (\sigma' \mid \eta) a \ \cup \ (\sigma \mid \eta') b \subseteq [\![\Delta]\!]$.

- $(\to)/(\twoheadrightarrow)$. For some σ', η', a, b, such that $\sigma = \sigma' a$ and $\eta \in \eta' \mid b$, we have:

$$\frac{\alpha \to a \in \Delta \qquad \sigma' \in [\![\Delta]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma'}}{\sigma' \, a \in [\![\Delta]\!]} \qquad \frac{\beta \twoheadrightarrow b \in \Delta \qquad \eta' \in [\![\Delta, b]\!] \qquad \overline{\beta} \subseteq \overline{\eta'}}{\eta' \mid b \subseteq [\![\Delta]\!]}$$

  Since $\sigma \in [\![\Delta]\!]$, then by Lemma 3.8 we also have $\sigma \in [\![\Delta, b]\!]$. We now apply the induction hypothesis twice: by the premise $\sigma' \in [\![\Delta]\!]$ and by $\eta \in [\![\Delta]\!]$, we obtain $\sigma' \mid \eta \subseteq [\![\Delta]\!]$; by the premise $\eta' \in [\![\Delta, b]\!]$ and by $\sigma \in [\![\Delta, b]\!]$, we obtain $\sigma \mid \eta' \subseteq [\![\Delta, b]\!]$. By applying the rules $(\to)$ and $(\twoheadrightarrow)$, we have:

$$\begin{aligned} \alpha \to a, \quad \sigma' \mid \eta \subseteq [\![\Delta]\!], \quad (\forall \tau \in \sigma' \mid \eta. \ \overline{\alpha} \subseteq \overline{\tau}) \implies (\sigma' \mid \eta) \, a \subseteq [\![\Delta]\!] \\ \beta \twoheadrightarrow b, \quad \sigma \mid \eta' \subseteq [\![\Delta, b]\!], \quad (\forall \tau \in \sigma \mid \eta'. \ \overline{\beta} \subseteq \overline{\tau}) \implies (\sigma \mid \eta') \mid b \subseteq [\![\Delta]\!] \end{aligned}$$

  The thesis follows because $\sigma \mid \eta \subseteq (\sigma' a) \mid (\eta' \mid b) = (\sigma' \mid \eta) a \ \cup \ (\sigma \mid \eta' \mid b) \subseteq [\![\Delta]\!]$.

- $(\twoheadrightarrow)/(\twoheadrightarrow)$. Similar to the previous case. □

Lemma 3.11. *For all Horn* PCL *theories* Δ*:*

(a) $\sigma \in [\![\Delta]\!] \implies \forall a \in \overline{\sigma}. \ \Delta \vdash a$

(b) $\forall a \in \overline{\sigma}. \ \Delta \vdash a \implies \exists \eta \in [\![\Delta]\!]. \ \overline{\sigma} \subseteq \overline{\eta}$

Proof. We first rewrite the statements in the following (equivalent) form:

(a) $\sigma \in [\![\Delta]\!] \implies \forall a \in \overline{\sigma}. \ \Delta \vdash a$

(b) $\Delta \vdash \alpha \implies \exists \eta \in [\![\Delta]\!]. \ \overline{\alpha} \subseteq \overline{\eta}$

Item (a) is shown by induction on the depth of the derivation of $\sigma \in [\![\Delta]\!]$. We have the following cases, according to the last rule used in the derivation.

- (ε). Trivial, because $\overline{\varepsilon} = \emptyset$.
- ($\to$). For some β, b, η such that $\sigma = \eta b$, we have that:

$$\frac{\beta \to b \in \Delta \qquad \eta \in [\![\Delta]\!] \qquad \overline{\beta} \subseteq \overline{\eta}}{\eta\, b \in [\![\Delta]\!]}$$

  Let $a \in \overline{\sigma} = \overline{\eta} \cup \{b\}$. We have two cases. If $a \in \overline{\eta}$, then the thesis follows directly from the induction hypothesis. Otherwise, if $a = b$, then by the induction hypothesis we have that $\forall b' \in \overline{\eta}.\ \Delta \vdash b'$. Since $\overline{\beta} \subseteq \overline{\eta}$, then by rule ($\wedge$I) we deduce $\Delta \vdash \beta$. Thus, by rule ($\to$E) we obtain the thesis:

$$\frac{\Delta \vdash \beta \to b \qquad \Delta \vdash \beta}{\Delta \vdash b}$$

- ($\twoheadrightarrow$). For some β, b and η such that $\sigma \in \eta \mid b$, we have:

$$\frac{\beta \twoheadrightarrow b \in \Delta \qquad \eta \in [\![\Delta, b]\!] \qquad \overline{\beta} \subseteq \overline{\eta}}{\eta \mid b \subseteq [\![\Delta]\!]}$$

  Let $a \in \overline{\sigma} = \overline{\eta} \cup \{b\}$. We first deal with the case $a = b$, by proving that $\Delta \vdash b$. By the induction hypothesis, we have that $\forall b' \in \overline{\eta}.\ \Delta, b \vdash b'$. By rule ($\wedge$I), this gives $\Delta, b \vdash \bigwedge \overline{\eta}$; also, since $\overline{\beta} \subseteq \overline{\eta}$, by introducing/eliminating conjunctions we deduce $\Delta, b \vdash \beta$. Thus, by rule ($\twoheadrightarrow$E) we conclude:

$$\frac{\Delta \vdash \beta \twoheadrightarrow b \qquad \Delta, b \vdash \beta}{\Delta \vdash b}$$

  Since $\Delta \vdash b$ and $\Delta, b \vdash \bigwedge \overline{\eta}$, then by the Cut Lemma (Lemma A.1) we conclude that $\Delta \vdash \bigwedge \overline{\eta}$. This gives the thesis for the case $a \in \overline{\eta}$.

Item (b) is shown by induction on the height of the proof of $\Delta \vdash \alpha$. By Lemma 3.4, we only have to consider the following cases, according to the last rule used in the proof:

- (ID). We have $\Delta \vdash a$, with $\Delta = \Delta', a = \Delta', \top \to a$ and $\alpha = a$. We have:

$$\frac{\top \to a \in \Delta \qquad \dfrac{}{\varepsilon \in [\![\Delta]\!]}\,(\varepsilon) \qquad \overline{\top} = \emptyset \subseteq \overline{\varepsilon}}{a = \varepsilon a \in [\![\Delta]\!]}\,(\to)$$

- ($\wedge$I). We have $\alpha = \alpha_1 \wedge \alpha_2$, where:

$$\frac{\Delta \vdash \alpha_1 \qquad \Delta \vdash \alpha_2}{\Delta \vdash \alpha_1 \wedge \alpha_2}$$

  By applying twice the induction hypothesis, we find $\eta_1 \in [\![\Delta]\!]$ and $\eta_2 \in [\![\Delta]\!]$ such that $\overline{\alpha_1} \subseteq \overline{\eta_1}$ and $\overline{\alpha_2} \subseteq \overline{\eta_2}$. Then, by Lemma 3.10 we have $\eta_1 \mid \eta_2 \subseteq [\![\Delta]\!]$. Let $\eta \in \eta_1 \mid \eta_2$. The thesis follows because $\overline{\alpha_1 \wedge \alpha_2} = \overline{\alpha_1} \cup \overline{\alpha_2} \subseteq \overline{\eta_1} \cup \overline{\eta_2} = \overline{\eta}$.

- ($\wedge$E1). We have:

$$\frac{\Delta \vdash \alpha \wedge \beta}{\Delta \vdash \alpha}$$

  By the induction hypothesis, there exists $\eta \in [\![\Delta]\!]$ such that $\overline{\alpha} \cup \overline{\beta} \subseteq \overline{\eta}$. The case for ($\wedge$E2) is similar.

- ($\to$E). We have $\alpha = a$, and:

$$\frac{\Delta \vdash \beta \to a \qquad \Delta \vdash \beta}{\Delta \vdash a}$$

  By the induction hypothesis, there exists $\eta' \in [\![\Delta]\!]$ such that $\overline{\beta} \subseteq \overline{\eta'}$. Then, by rule ($\to$):

$$\frac{\beta \to a \in \Delta \qquad \eta' \in [\![\Delta]\!] \qquad \overline{\beta} \subseteq \overline{\eta'}}{\eta' a \in [\![\Delta]\!]}$$

  The thesis follows with $\eta = \eta' a$, because $\overline{\alpha} = \overline{a} \subseteq \overline{\eta}$.

- ($\twoheadrightarrow$E). We have $\alpha = a$, and
$$\frac{\Delta \vdash \beta \twoheadrightarrow a \qquad \Delta, a \vdash \beta}{\Delta \vdash a}$$
By the induction hypothesis, there exists $\eta' \in [\![\Delta, a]\!]$ such that $\overline{\beta} \subseteq \overline{\eta'}$. Then, by rule ($\twoheadrightarrow$):
$$\frac{\beta \twoheadrightarrow a \in \Delta \qquad \eta' \in [\![\Delta, a]\!] \qquad \overline{\beta} \subseteq \overline{\eta'}}{\eta' \mid a \in [\![\Delta]\!]}$$
The thesis follows by choosing any $\eta \in \eta' \mid a$, because $\overline{\alpha} = \overline{a} \subseteq \overline{\eta}$. □

Lemma 3.13. $\sigma\nu \in [\![\Delta]\!] \ \wedge \ \eta \in [\![\Delta, \overline{\sigma}]\!] \implies \sigma(\nu \mid \eta) \subseteq [\![\Delta]\!]$

Proof. By induction on the depth of the proof of $\sigma\nu \in [\![\Delta]\!]$. The base case is when the rule (ε) is applied. We have $\sigma = \nu = \varepsilon$, hence the thesis holds trivially.

For the inductive case, we have the following two subcases, according to the last rule used to deduce $\sigma\nu \in [\![\Delta]\!]$.

- ($\to$). We have $\sigma\nu = \tau a$, for some τ and a such that:
$$\frac{\alpha \to a \in \Delta \qquad \tau \in [\![\Delta]\!] \qquad \overline{\alpha} \subseteq \overline{\tau}}{\tau a \in [\![\Delta]\!]}$$
There are the following subcases:
  - $a \in \overline{\tau}$. Then, $\tau = \tau a = \sigma\nu$. Hence, the thesis follows directly by the induction hypothesis.
  - $a \notin \overline{\tau}$, $\nu = \varepsilon$. By Lemma 3.9, we have that $\sigma\eta \in [\![\Delta]\!]$. The thesis follows because $\sigma(\nu \mid \eta) = \sigma(\varepsilon \mid \eta) = \sigma\eta$.
  - $a \notin \overline{\tau}$, $\nu \neq \varepsilon$. Then, $\tau = \sigma\nu'$, with $\nu = \nu' a$. By the induction hypothesis, $\sigma(\nu' \mid \eta) \subseteq [\![\Delta]\!]$. By hypothesis, we also have $\tau a = \sigma\nu' a \in [\![\Delta]\!]$. By Lemma 3.10 we have $\big(\sigma(\nu' \mid \eta)\big) \mid \sigma\nu' a \subseteq [\![\Delta]\!]$. The thesis follows because $\sigma(\nu \mid \eta) = \sigma(\nu' a \mid \eta) = \sigma(\nu' \mid \eta \mid \nu' a) = \big(\sigma(\nu' \mid \eta)\big) \mid \sigma\nu' a \subseteq [\![\Delta]\!]$.
- ($\twoheadrightarrow$). We have $\sigma\nu \in \tau \mid a$, for some τ and a such that:
$$\frac{\alpha \twoheadrightarrow a \in \Delta \qquad \tau \in [\![\Delta, a]\!] \qquad \overline{\alpha} \subseteq \overline{\tau}}{\tau \mid a \subseteq [\![\Delta]\!]}$$
There are the following subcases:
  - $a \in \overline{\sigma}$. We have that $\tau = \sigma'\nu$, for some $\sigma' \in \sigma \mid a$. Since $\sigma'\nu \in [\![\Delta, a]\!]$ and $\eta \in [\![\Delta, \overline{\sigma}]\!] = [\![\Delta, a, \overline{\sigma'}]\!]$ then by the induction hypothesis it follows that $\sigma'(\nu \mid \eta) \subseteq [\![\Delta, a]\!]$. Then, by rule ($\twoheadrightarrow$) we obtain $\sigma'(\nu \mid \eta) \mid a \subseteq [\![\Delta]\!]$. The thesis follows because $\sigma(\nu \mid \eta) \subseteq \sigma'(\nu \mid \eta) \mid a \subseteq [\![\Delta]\!]$.
  - $a \notin \overline{\sigma}$, $a \in \overline{\nu}$. We have that $\tau = \sigma\nu'$, for some $\nu' \in \nu \mid a$. Since $\sigma\nu' \in [\![\Delta, a]\!]$ and $\eta \in [\![\Delta, \overline{\sigma}]\!] \subseteq [\![\Delta, a, \overline{\sigma}]\!]$, then by the induction hypothesis it follows that $\sigma(\nu' \mid \eta) \subseteq [\![\Delta, a, \overline{\sigma}]\!]$. Let $\tau' \in \sigma(\nu' \mid \eta)$. Then, by rule ($\twoheadrightarrow$), it follows that $\tau' \mid a \subseteq [\![\Delta]\!]$. Summing up, $\sigma(\nu' \mid \eta) \mid a \subseteq [\![\Delta]\!]$. The thesis follows because $\sigma(\nu \mid \eta) \subseteq \sigma(\nu' \mid \eta) \mid a \subseteq [\![\Delta]\!]$. □

Lemma 3.18. *For all Horn* PCL *theories* Δ*, for all* $\Gamma \subseteq {!}E \cup UE$*, and for all* α*:*

$$[\Delta]_{\mathcal{U}}, \Gamma \vdash \alpha \implies \begin{cases} \overline{\alpha}^R \ \subseteq \ \bigcup \overline{[\![\Delta, \overline{\Gamma}^{!U}]\!]} & \text{(5a)} \\ \overline{\alpha}^U \ \subseteq \ \mathcal{U}^{\overline{\Gamma}^!}_{\Delta, \overline{\Gamma}^U} \cup \overline{\Gamma}^{!U} & \text{(5b)} \end{cases}$$

Proof. By induction on the depth of the proof of $[\Delta]_{\mathcal{U}}, \Gamma \vdash \alpha$.

The base case concerns the axiom (ID), for which we have $[\Delta]_{\mathcal{U}}, \Gamma', \star a \vdash \star a$, with $\star \in \{!, U\}$ and $\Gamma = \Gamma', \star a$. We have the following two subcases:

- $\star = !$. We have $\overline{!a}^R = \overline{!a}^U = \emptyset$, so both (5a) and (5b) hold trivially.
- $\star = U$. We have $\overline{Ua}^R = \emptyset$, so (5a) is trivial. For (5b) we have $\overline{Ua}^U = \{a\}$, hence the thesis follows by $\overline{Ua}^U = \{a\} \subseteq \overline{\Gamma}^U \subseteq \mathcal{U}^{\overline{\Gamma}^!}_{\Delta,\overline{\Gamma}^U} \cup \overline{\Gamma}^{!U}$.

For the inductive case, we analyse the last rule used in the proof of $[\Delta]_\mathcal{U}, \Gamma \vdash \alpha$. According to Lemma 3.4, there are the following exhaustive cases:

- ($\to$E). We have that $\alpha = q$, for some p and q such that:

$$\frac{[\Delta]_\mathcal{U}, \Gamma \vdash p \to q \qquad [\Delta]_\mathcal{U}, \Gamma \vdash p}{[\Delta]_\mathcal{U}, \Gamma \vdash q}$$

  By Definition 3.16, the formula $p \to q \in [\Delta]_\mathcal{U}$ has one of the following forms:

  - $!a \to Ua$. For (5a) the thesis follows trivially, because $\overline{Ua}^R = \emptyset$.
    For (5b), we have $\overline{Ua}^U = \{a\}$. If $a \in \overline{\Gamma}^!$, we already have the thesis. Otherwise, if $a \notin \overline{\Gamma}^!$, then $[\Delta]_\mathcal{U}, \Gamma \not\vdash !a$, hence the premise that $!a \to Ua$ is eliminated through rule ($\to$E) must be false.
  - $!\overline{\beta} \to Ua$. This has been generated by an implication $\beta \to a \in \Delta$.
    For (5a), we have that $\overline{Ua}^R = \emptyset$, hence the thesis follows trivially.
    For (5b), we have that $\overline{Ua}^U = \{a\}$. There are two further subcases. If $a \in \overline{\Gamma}^!$, we already have the thesis. Otherwise, assume $a \notin \overline{\Gamma}^!$. By the second premise of rule ($\to$E), we have $[\Delta]_\mathcal{U}, \Gamma \vdash !\overline{\beta}$. By Definition 3.16, the encoding $[\cdot]_\mathcal{U}$ cannot introduce !-atoms, hence it must be $\overline{\Gamma}^! \vdash \overline{\beta}$. By Lemma 3.11(b), there exists $\eta \in [\![\overline{\Gamma}^!]\!]$ such that $\overline{\beta} \subseteq \overline{\eta}$, and so by Lemma 3.8, $\eta \in [\![\Delta, \overline{\Gamma}^!]\!]$. Then, by rule ($\to$):

$$\frac{\beta \to a \in \Delta \qquad \eta \in [\![\Delta, \overline{\Gamma}^!]\!] \qquad \overline{\beta} \subseteq \overline{\eta}}{\eta a \in [\![\Delta, \overline{\Gamma}^!]\!]}$$

    Clearly, we also have $\overline{\Gamma}^! \vdash \overline{\Gamma}^!$, then by Lemma 3.11(b) and by Lemma 3.8 we find some $\nu \in [\![\Delta, \overline{\Gamma}^!]\!]$ (such that $\overline{\nu} \supseteq \overline{\Gamma}^!$). Therefore, by Lemma 3.10:

$$\eta a \mid \nu \ \subseteq \ [\![\Delta, \overline{\Gamma}^!]\!]$$

    from which (using Lemma 3.8 to justify the last inclusion) we deduce that:

$$\exists \sigma, \sigma'.\ \overline{\sigma} = \overline{\Gamma}^! \ \wedge\ \sigma\, a\, \sigma' \in \eta a \mid \nu \subseteq [\![\Delta]\!] \subseteq [\![\Delta, \overline{\Gamma}^U]\!]$$

    Since $a \notin \overline{\Gamma}^!$, by Definition 3.14 we obtain the thesis $a \in \mathcal{U}^{\overline{\Gamma}^!}_{\Delta,\overline{\Gamma}^U}$.
  - $R\overline{\beta} \to Ra$. This has been generated by an implication $\beta \to a \in \Delta$.
    For (5a), we have that $\overline{Ra}^R = \{a\}$. By the second premise of rule ($\to$E), it must be $[\Delta]_\mathcal{U}, \Gamma \vdash R\overline{\beta}$. By the induction hypothesis of (5a), it follows that:

$$\overline{\beta} \ = \ \overline{\overline{R\overline{\beta}}^R} \ \subseteq \ \bigcup \overline{[\![\Delta, \overline{\Gamma}^{!U}]\!]} \tag{6}$$

    Let $\overline{\beta} = \{b_1, \ldots, b_n\}$. By (6), for all $i \in 1..n$ there exists $\eta^i \in [\![\Delta, \overline{\Gamma}^{!U}]\!]$ such that $b_i \in \overline{\eta^i}$. By Lemma 3.10, we have that $\eta^1 \mid \cdots \mid \eta^n \subseteq [\![\Delta, \overline{\Gamma}^{!U}]\!]$. Let $\eta \in \eta^1 \mid \cdots \mid \eta^n$. Then, $\overline{\beta} \subseteq \overline{\eta}$, and so by rule ($\to$) we have:

$$\frac{\beta \to a \in \Delta \qquad \eta \in [\![\Delta, \overline{\Gamma}^{!U}]\!] \qquad \overline{\beta} \subseteq \overline{\eta}}{\eta a \in [\![\Delta, \overline{\Gamma}^{!U}]\!]}$$

    from which the thesis follows, because $a \in \overline{\eta a}$.
    For (5b), the thesis follows trivially because $\overline{Ra}^U = \emptyset$.

– $Ua \to Ra$. For (5a), we have $\overline{Ra}^R = \{a\}$. By the second premise of rule (→E), it must be $[\Delta]_{\mathcal{U}}, \Gamma \vdash Ua$. Therefore, by the induction hypothesis of (5b):

$$\{a\} \;=\; \overline{Ua}^U \;\subseteq\; \mathcal{U}^{\overline{\Gamma}^!}_{\Delta,\overline{\Gamma}^U} \cup \Gamma^{!U}$$

Now we have the following two subcases:

1. $a \in \overline{\Gamma}^{!U}$. Therefore, $\Delta, \overline{\Gamma}^{!U} \vdash a$. By Lemma 3.11(b) we find some $\sigma \in [\![\Delta, \overline{\Gamma}^{!U}]\!]$ such that $a \in \overline{\sigma}$, from which the thesis follows.
2. $a \in \mathcal{U}^{\overline{\Gamma}^!}_{\Delta,\overline{\Gamma}^U}$. By Definition 3.14, $a \notin \overline{\Gamma}^!$, and there exist σ, σ' such that $\overline{\sigma} = \overline{\Gamma^!}$ and $\sigma\, a\, \sigma' \in [\![\Delta, \overline{\Gamma}^U]\!]$, from which the thesis follows (notice that $[\![\Delta, \overline{\Gamma}^U]\!] \subseteq [\![\Delta, \overline{\Gamma}^{!U}]\!]$ by Lemma 3.8).

For (5b), the thesis follows trivially because $\overline{Ra}^U = \emptyset$.

- (→E). By Definition 3.16, it must be $\alpha = Ua$, for some a and β such that:

$$\frac{[\Delta]_{\mathcal{U}}, \Gamma, \vdash R\beta \twoheadrightarrow Ua \qquad [\Delta]_{\mathcal{U}}, \Gamma, Ua \vdash R\beta}{[\Delta]_{\mathcal{U}}, \Gamma \vdash Ua}$$

where $R\beta \twoheadrightarrow Ua \in [\Delta]_{\mathcal{U}}$ has been generated by $\beta \twoheadrightarrow a \in \Delta$.

For (5a), the thesis follows trivially, because $\overline{Ua}^R = \emptyset$.

For (5b), we have that $\overline{Ua}^U = \{a\}$. If $a \in \overline{\Gamma}^!$, we already have the thesis. Otherwise, assume $a \notin \overline{\Gamma}^!$. By the second premise of rule (→E) we have $[\Delta]_{\mathcal{U}}, \Gamma' \vdash R\beta$, where $\Gamma' = \Gamma \cup \{Ua\}$. Then, by the induction hypothesis of (5a), it follows that:

$$\overline{\beta} \;=\; \overline{R\beta}^R \;\subseteq\; \bigcup \overline{[\![\Delta, \overline{\Gamma'}^{!U}]\!]} \;=\; \bigcup \overline{[\![\Delta, \overline{\Gamma}^{!U}, a]\!]} \tag{7}$$

Let $\overline{\beta} = \{b_1, \ldots, b_n\}$. By (7), for all $i \in 1..n$ there exists $\eta^i \in [\![\Delta, \overline{\Gamma}^{!U}, a]\!]$ such that $b_i \in \overline{\eta^i}$. By Lemma 3.10, we have that $\eta^1 \mid \cdots \mid \eta^n \subseteq [\![\Delta, \overline{\Gamma}^{!U}, a]\!]$. Let $\eta \in \eta^1 \mid \cdots \mid \eta^n$. Then, $\overline{\beta} \subseteq \overline{\eta}$, and so by rule (→) we have:

$$\frac{\beta \twoheadrightarrow a \in \Delta \qquad \eta \in [\![\Delta, \overline{\Gamma}^{!U}, a]\!] \qquad \overline{\beta} \subseteq \overline{\eta}}{\eta \mid a \subseteq [\![\Delta, \overline{\Gamma}^{!U}]\!]}$$

Clearly, we also have $\overline{\Gamma}^! \vdash \overline{\Gamma}^!$, then by Lemma 3.11(b) and by Lemma 3.8 we find some $\nu \in [\![\Delta, \overline{\Gamma}^{!U}]\!]$ (such that $\overline{\nu} = \overline{\Gamma}^!$). Therefore, by Lemma 3.10:

$$\eta \mid a \mid \nu \;\subseteq\; [\![\Delta, \overline{\Gamma}^{!U}]\!]$$

from which we deduce that:

$$\exists \sigma, \sigma'.\ \overline{\sigma} = \overline{\Gamma}^! \;\wedge\; \sigma a \sigma' \in \eta \mid a \mid \nu \subseteq [\![\Delta, \overline{\Gamma}^{!U}]\!]$$

Since $a \notin \overline{\Gamma}^!$, we obtain the thesis $a \;\in\; \mathcal{U}^{\overline{\Gamma}^!}_{\Delta,\overline{\Gamma}^{!U}} \;=\; \mathcal{U}^{\overline{\Gamma}^!}_{\Delta,\overline{\Gamma}^U}$.

- (∧I), (∧E). Both cases are straightforward by the induction hypothesis. □

Lemma 3.19. $a \in \bigcup \overline{[\![\Delta]\!]} \iff [\Delta]_{\mathcal{U}} \vdash Ra$

Proof. For (⇒) we prove the following statement, which implies the thesis:

$$\sigma \in [\![\Delta]\!] \implies [\Delta]_{\mathcal{U}} \vdash R\overline{\sigma}$$

We proceed by induction on the depth of the derivation $\sigma \in [\![\Delta]\!]$. According to the last rule used in the derivation, there are the following cases:

- (ε). We have $\varepsilon \in [\![\Delta]\!]$. The thesis follows trivially, because $R\overline{\varepsilon} = R\emptyset = \top$.
- ($\to$). We have $\sigma = \sigma' a$, for some σ' and a such that:

$$\frac{\alpha \to a \in \Delta \qquad \sigma' \in [\![\Delta]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma'}}{\sigma' a \in [\![\Delta]\!]}$$

  By the induction hypothesis, $[\Delta]_{\mathcal{U}} \vdash R\overline{\sigma'}$. Since $\overline{\alpha} \subseteq \overline{\sigma'}$, it follows that $[\Delta]_{\mathcal{U}} \vdash R\overline{\alpha}$. Since $\alpha \to a \in \Delta$, then by Definition 3.16 we have $[\Delta]_{\mathcal{U}} \vdash R\overline{\alpha} \to Ra$. Therefore, by rule ($\to$E) we can deduce $[\Delta]_{\mathcal{U}} \vdash Ra$, from which the thesis follows.
- ($\twoheadrightarrow$). We have $\sigma \in \sigma' \mid a$ for some σ' and a such that:

$$\frac{\alpha \twoheadrightarrow a \in \Delta \qquad \sigma' \in [\![\Delta, a]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma'}}{\sigma' \mid a \subseteq [\![\Delta]\!]}$$

  By the induction hypothesis we have $[\Delta, a]_{\mathcal{U}} \vdash R\overline{\sigma'}$, and since $\overline{\alpha} \subseteq \overline{\sigma'}$ by the third premise of rule ($\twoheadrightarrow$E), it follows that $[\Delta]_{\mathcal{U}}, Ra \vdash R\overline{\alpha}$. By Definition 3.16 we have $Ua \to Ra \in \Omega(\Delta)$, hence $[\Delta]_{\mathcal{U}} \vdash Ua \to Ra$. Therefore, we can weaken the above to $[\Delta]_{\mathcal{U}}, Ua \vdash R\overline{\alpha}$. Now, since $\alpha \twoheadrightarrow a \in \Delta$, then $[\Delta]_{\mathcal{U}} \vdash R\overline{\alpha} \twoheadrightarrow Ua$. By rule ($\twoheadrightarrow$E):

$$\frac{[\Delta]_{\mathcal{U}} \vdash R\overline{\alpha} \twoheadrightarrow Ua \qquad [\Delta]_{\mathcal{U}}, Ua \vdash R\overline{\alpha}}{[\Delta]_{\mathcal{U}} \vdash Ua}$$

  from which by rule ($\to$E) we obtain the thesis:

$$\frac{[\Delta]_{\mathcal{U}} \vdash Ua \to Ra \qquad [\Delta]_{\mathcal{U}} \vdash Ua}{[\Delta]_{\mathcal{U}} \vdash Ra}$$

For ($\Leftarrow$) the thesis follows directly by item (5a) of Lemma 3.18. □

Lemma A.3. *For all sets of atoms X, for all atoms a, and for $\star \in \{!, U\}$:*

$$[\Delta]_{\mathcal{U}}, \star X \vdash Ra \implies [\Delta]_{\mathcal{U}}, RX \vdash Ra$$

Proof. We first show the following result. For all $X \subseteq E$:

$$\Delta, X \vdash a \quad \Longrightarrow \quad [\Delta]_{\mathcal{U}}, RX \vdash Ra \tag{8}$$

To prove (8) we proceed by induction on the depth of the proof of $\Delta, X \vdash a$. If the last rule used is ($\twoheadrightarrow$E), we have that $\alpha = a$, and, for some β:

$$\frac{\Delta, X \vdash \beta \twoheadrightarrow a \qquad \Delta, X, a \vdash \beta}{\Delta, X \vdash a}$$

Since $\beta \twoheadrightarrow a \in \Delta$, then by Definition 3.16 we have that $R\overline{\beta} \twoheadrightarrow Ua \in [\Delta]_{\mathcal{U}}$. By the induction hypothesis (applied to the second premise of the ($\twoheadrightarrow$E) rule), we have that $[\Delta]_{\mathcal{U}}, RX, Ra \vdash R\overline{\beta}$. Since $Ua \to Ra \in [\Delta]_{\mathcal{U}}$, this can be weakened to $[\Delta]_{\mathcal{U}}, RX, Ua \vdash R\overline{\beta}$. Summing up, we have the following derivation:

$$\dfrac{[\Delta]_{\mathcal{U}}, RX \vdash Ua \to Ra \qquad \dfrac{[\Delta]_{\mathcal{U}}, RX \vdash R\overline{\beta} \twoheadrightarrow Ua \qquad [\Delta]_{\mathcal{U}}, RX, Ua \vdash R\overline{\beta}}{[\Delta]_{\mathcal{U}}, RX \vdash Ua}\,(\twoheadrightarrow\text{E})}{[\Delta]_{\mathcal{U}}, RX \vdash Ra}\,(\to\text{E})$$

All the other cases (for the last rule used to derive $\Delta, X \vdash \alpha$) are straightforward.

Back to the main statement of Lemma A.3, we consider separately the cases where $\star = U$ and $\star =!$.

- case $\star = U$. Assume that $[\Delta]_{\mathcal{U}}, UX \vdash Ra$. By Definition 3.16, this is equivalent to $[\Delta, X]_{\mathcal{U}}, \vdash Ra$. By Lemma 3.19, $a \in \bigcup \overline{[\![\Delta, X]\!]}$. By Lemma 3.11, $\Delta, X \vdash a$. Then, by (8) we conclude that $[\Delta]_{\mathcal{U}}, RX \vdash Ra$.

- case $\star =!$. We first show that, for $\triangleright \in \{!, U, R\}$:

$$[\Delta]_{\mathcal{U}}, !X \vdash \triangleright\, a \quad \Longrightarrow \quad \Delta, X \vdash a \tag{9}$$

  This is done easily by induction on the depth of the proof of $[\Delta]_{\mathcal{U}}, !X \vdash \triangleright\ a$. Now, assume that $[\Delta]_{\mathcal{U}}, !X \vdash Ra$. By (9), we have $\Delta, X \vdash a$. By (8), we conclude that $[\Delta]_{\mathcal{U}}, RX \vdash Ra$.

□

Lemma 3.20. *Let $\sigma = \langle e_0 \cdots e_n \rangle$. Then,*

$$\forall i \in 0..n.\ [\Delta]_{\mathcal{U}},\ !\overline{\sigma_i} \vdash Ue_i \quad \Longleftrightarrow \quad \exists \eta.\ \sigma\eta \in [\![\Delta]\!]$$

Proof. For ($\Leftarrow$), without loss of generality we can show that:

$$\forall i \in 0..n.\ [\Delta]_{\mathcal{U}},\ !\overline{\sigma_i} \vdash Ue_i \quad \Longleftarrow \quad \sigma \in [\![\Delta]\!]$$

We proceed by induction on the length of σ. The base case $\sigma = \varepsilon$ is trivial. For the inductive case, we have the following cases according to the last rule used in the derivation of $\sigma \in [\![\Delta]\!]$.

- ($\rightarrow$) We have $\sigma = \sigma_n e_n$, where

$$\frac{\alpha \to e_n \in \Delta \qquad \sigma_n \in [\![\Delta]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma_n}}{\sigma_n e_n \in [\![\Delta]\!]}$$

  By the induction hypothesis, we have that $\forall i \in 0..n-1.\ [\Delta]_{\mathcal{U}},\ !\overline{\sigma_i} \vdash Ue_i$. Since $\sigma = \sigma_n e_n$, it remains to prove that $[\Delta]_{\mathcal{U}},\ !\overline{\sigma} \vdash Ue_n$. Since $\overline{\alpha} \subseteq \overline{\sigma_n}$, we deduce that $[\Delta]_{\mathcal{U}},\ !\overline{\sigma} \vdash\ !\overline{\alpha}$. Since $\alpha \to e_n \in \Delta$, then by Definition 3.16 we have $[\Delta]_{\mathcal{U}},\ !\overline{\sigma} \vdash\ !\overline{\alpha} \to Ue_n$. Then, by rule ($\to$E) we have the thesis:

$$\frac{[\Delta]_{\mathcal{U}},\ !\overline{\sigma} \vdash\ !\overline{\alpha} \to Ue_n \qquad [\Delta]_{\mathcal{U}},\ !\overline{\sigma} \vdash\ !\overline{\alpha}}{[\Delta]_{\mathcal{U}},\ !\overline{\sigma} \vdash Ue_n}$$

- ($\twoheadrightarrow$). We have $\sigma \in \sigma' \mid e_k$, where $\sigma' = \langle e'_0 \cdots e'_{n-1} \rangle = \langle e_0 \cdots e_{k-1}\, e_{k+1} \cdots e_n \rangle$, and:

$$\frac{\alpha \twoheadrightarrow e_k \in \Delta \qquad \sigma' \in [\![\Delta, e_k]\!] \qquad \overline{\alpha} \subseteq \overline{\sigma'}}{\sigma' \mid e_k \subseteq [\![\Delta]\!]}$$

  By the induction hypothesis we have that $\forall i \in 0..n-1.\ [\Delta, e_k]_{\mathcal{U}},\ !\overline{\sigma'_i} \vdash Ue'_i$. By Definition 3.16, this is equivalent to $\forall i \in 0..n-1.\ [\Delta]_{\mathcal{U}}, Ue_k,\ !\overline{\sigma'_i} \vdash Ue'_i$. Since $\overline{\sigma} = \overline{\sigma'} \cup \{e_k\}$ and $!e_k \to Ue_k \in [\Delta]_{\mathcal{U}}$, this implies that $\forall i \neq k.\ [\Delta]_{\mathcal{U}},\ !\overline{\sigma_i} \vdash Ue_i$. Then, it remains to prove that $[\Delta]_{\mathcal{U}},\ !\overline{\sigma_k} \vdash Ue_k$. Since $\overline{\alpha} \subseteq \overline{\sigma}$, we have that $[\Delta, e_k]_{\mathcal{U}},\ !\overline{\sigma} \vdash\ !\overline{\alpha}$, hence by Definition 3.16:

$$[\Delta]_{\mathcal{U}}, !\overline{\sigma}, Ue_k \vdash\ !\overline{\alpha} \tag{10}$$

  By Definition 3.16 we have $!\overline{\alpha} \to U\overline{\alpha} \in [\Delta]_{\mathcal{U}}$ and $U\overline{\alpha} \to R\overline{\alpha} \in [\Delta]_{\mathcal{U}}$, hence by (10) it follows that:

$$[\Delta]_{\mathcal{U}}, !\overline{\sigma}, Ue_k \vdash R\overline{\alpha}$$

  By Lemma A.3, it follows that

$$[\Delta]_{\mathcal{U}}, !\overline{\sigma_k}, R\overline{\sigma}, Ue_k \vdash R\overline{\alpha}$$

  Since $\sigma \in [\![\Delta]\!]$, then by Lemma 3.19 it follows that $[\Delta]_{\mathcal{U}} \vdash R\overline{\sigma}$. Then by Lemma A.1:

$$[\Delta]_{\mathcal{U}}, !\overline{\sigma_k}, Ue_k \vdash R\overline{\alpha}$$

  Since $\alpha \twoheadrightarrow e_k \in \Delta$, then by Definition 3.16 we have $R\overline{\alpha} \twoheadrightarrow Ue_k \in [\Delta]_{\mathcal{U}}$. Then by rule ($\twoheadrightarrow$E) we conclude:

$$\frac{[\Delta]_{\mathcal{U}}, !\overline{\sigma_k} \vdash R\overline{\alpha} \twoheadrightarrow Ue_k \qquad [\Delta]_{\mathcal{U}}, !\overline{\sigma_k}, Ue_k \vdash R\overline{\alpha}}{[\Delta]_{\mathcal{U}},\ !\overline{\sigma_k} \vdash Ue_k}$$

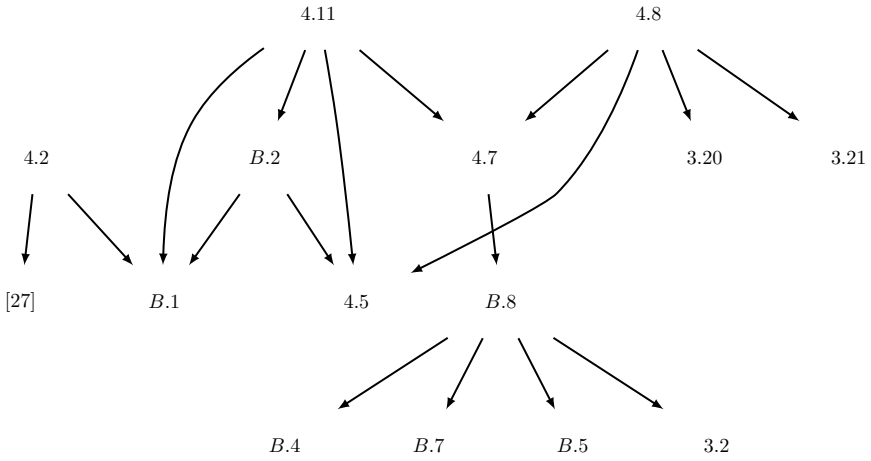

Figure 10: Dependencies among the proofs.

For ($\Rightarrow$), assume that $[\Delta]_{\mathcal{U}}$, $!\overline{\sigma_i} \vdash Ue_i$, for all $i \in 0..n$. By item (5b) of Lemma 3.18, it follows that:

$$\forall i \in 0..n.\ \ e_i \in \mathcal{U}^{\overline{\sigma_i}}_{\Delta,\overline{\sigma_i}} \cup !\overline{\sigma_i}^{!U}$$

Notice that $e_i \notin \overline{\sigma_i} = !\overline{\sigma_i}^{!U}$, hence

$$\forall i \in 0..n.\ \ e_i \in \mathcal{U}^{\overline{\sigma_i}}_{\Delta,\overline{\sigma_i}}$$

By Definition 3.14, this means that:

$$\forall i \in 0..n.\ \ \exists \eta^i, \nu^i.\ \ \overline{\eta^i} = \overline{\sigma_i} \ \wedge\ \eta^i e_i \nu^i \in [\![\Delta, \overline{\sigma_i}]\!] \tag{11}$$

We construct a proof trace $\sigma\eta \in [\![\Delta]\!]$ as follows. Start with the first two elements in σ. By (11), we have:

$$\eta^0\, e_0\, \nu^0 \in [\![\Delta, \overline{\sigma_0}]\!] \qquad \text{with } \overline{\eta^0} = \emptyset = \overline{\sigma_0}$$
$$\eta^1\, e_1\, \nu^1 \in [\![\Delta, \overline{\sigma_1}]\!] \qquad \text{with } \overline{\eta^1} = \{e_0\} = \overline{\sigma_1}$$

Since $\overline{\sigma_0} = \overline{\eta^0 e_0}$, then by Lemma 3.13, it follows that:

$$\eta^0\, e_0\, (\eta^1\, e_1\, \nu^1 \mid \nu^0) \ =\ e_0\, (e_1\, \nu^1 \mid \nu^0) \ \subseteq\ [\![\Delta]\!]$$

In particular, for some $\nu' \in \nu^1 \mid \nu^0$ we can choose a trace $\sigma^0 = e_0\, e_1\, \nu' \in [\![\Delta]\!]$. Repeating this procedure for all the elements in σ, we finally obtain some ν such that $\sigma\nu \in [\![\Delta]\!]$. □

B. Proofs for Section 4

The diagram in Figure 10 illustrates the dependencies among the proofs.

Lemma B.1. *Let $\mathcal{C}$ be a conflict-free contract, and let σ be a play of $\mathcal{C}$ where all participants are innocent. Then, $\overline{\sigma} = \mathcal{R}^{\emptyset}$.*

Proof. Special case (for conflict-free CES) of Lemma 5.15 in [27]. □

Lemma 4.5. *In finite conflict-free contracts, an event e is prudent in σ iff $e \in \mathcal{P}^{\overline{\sigma}}$.*

Proof. ($\Leftarrow$) We start by examining the coinductive definition of prudent events and innocent participants (Definition 2.12). We can regard such definition as determining a pair of relations (Pr, In), where $Pr \in \wp(E \times E^*)$ relates e and σ when e is prudent in σ, while $In \in \wp(\mathcal{A} \times E^\infty)$ relates A and σ when A s innocent in σ. Since the definition is coinductive, the pair (Pr, In) can be expressed as the greatest fixed point of an endofunction F operating as follows:

$$F : \wp(E \times E^*) \times \wp(\mathcal{A} \times E^\infty) \to \wp(E \times E^*) \times \wp(\mathcal{A} \times E^\infty)$$

Indeed, we can augment $L = \wp(E \times E^*) \times \wp(\mathcal{A} \times E^\infty)$ with the partial order given by $(P, I) \sqsubseteq (P', I')$ iff $P \subseteq P' \wedge I \supseteq I'$. It is immediate to check that this ordering makes L a complete lattice (in which $\bigsqcup_i (P_i, I_i) = (\bigcup_i P_i, \bigcap_i I_i)$). We can formalize the function F underlying Definition 2.12 letting $F(P, I) = (P', I')$ where:

$$\begin{aligned} P' = \{(e, \sigma) \mid \exists \Sigma.\ & \sigma e \text{ conform to } \Sigma \wedge \\ & \forall \sigma' = \sigma\, e\, \eta \text{ fair conform to } \Sigma.\ \big(\forall \mathsf{B} \neq \pi(e).\ (\mathsf{B}, \sigma') \in I\big) \\ & \implies \phi(\sigma, \sigma', \mathsf{A})\} \\ I' = \{(\mathsf{A}, \sigma) \mid \forall e \in \pi^{-1}(\mathsf{A}).\ & \forall i \in 0..|\sigma|.\ \exists j \geq i.\ (e, \sigma_j) \notin P\} \end{aligned}$$

with predicate ϕ being:

$$\phi(\sigma, \sigma', \mathsf{A}) \triangleq \exists k > |\sigma|.\ \Gamma(\sigma'_k) \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma)$$

Note that the above makes F monotonic with respect to $\sqsubseteq$. This ensures $\operatorname{gfp} F$ actually exists.

We now exploit the coinduction proof principle on the complete lattice L and function F to prove the current lemma. The coinduction principle states that, for all $x \in L$:

$$x \sqsubseteq F(x) \implies x \sqsubseteq \operatorname{gfp} F$$

To apply the above, we take $x = (P, I)$ where:

$$\begin{aligned} P &= \{(e, \sigma) \mid e \in \mathcal{P}^{\overline{\sigma}}\} \\ I &= \{(\mathsf{A}, \sigma) \mid \mathcal{P}^{\overline{\sigma}} \cap \pi^{-1}(\mathsf{A}) = \emptyset\} \end{aligned}$$

Then, the thesis "$e \in \mathcal{P}^{\overline{\sigma}} \implies e$ prudent in σ" follows from $x = (P, I) \sqsubseteq \operatorname{gfp} F$, since that implies that $P \subseteq Pr$. By the coinduction principle, we are left with proving $x \sqsubseteq F(x)$. Below, we let $(P', I') = F(x)$, and prove $P \subseteq P'$ and $I \supseteq I'$.

We first show $P \subseteq P'$. Let $(e, \sigma) \in P$, let $\sigma = \langle e_0 \cdots e_n \rangle$, and let $\mathsf{A} = \pi(e)$. The choice of the strategy Σ in P' is made as follows. For all η, let:

$$\Sigma_{\mathsf{A}}(\eta) = \begin{cases} \{e_i\} & \text{if } \eta = \sigma_i \text{ and } \pi(e_i) = \mathsf{A} \text{ and } i \in 0..n \\ \mathcal{P}^{\overline{\eta}} \cap \pi^{-1}(\mathsf{A}) & \text{otherwise} \end{cases}$$

Notice that, since the contract is conflict-free, then Σ_{A} is well-defined; also, by construction σ conforms to Σ_{A} (in other words, Σ_{A} has past σ). Let σ' be a fair play extending σe, conform to Σ_{A}, and such that $(\mathsf{B}, \sigma') \in I$ for all $\mathsf{B} \neq \mathsf{A}$. Since $(e, \sigma) \in P$, then $e \in \mathcal{P}^{\overline{\sigma}}$.

We need to prove that $\phi(\sigma, \sigma', \mathsf{A})$. For this, recall that E is finite, so σ' must be finite as well. This allows us to take $k = |\sigma'| > |\sigma|$, leaving us to prove that $\Gamma(\sigma'_k) \cap \pi^{-1}(\mathsf{A}) = \Gamma(\sigma') \cap \pi^{-1}(\mathsf{A}) \subseteq \Gamma(\sigma)$. Assume by contradiction that there exists $e' \in (\Gamma(\sigma') \cap \pi^{-1}(\mathsf{A})) \setminus \Gamma(\sigma)$. This implies that $\sigma' = \sigma \eta e' \eta'$ for some η, η'. Since σ' is conform to Σ_{A}, we must have $e' \in \mathcal{P}^{\overline{\sigma\eta}}$, implying by definition of $\mathcal{P}$:

$$\overline{\sigma\eta} \vdash e' \qquad \vee \qquad \overline{\sigma\eta} \cup \mathcal{R}^{\overline{\sigma\eta}} \Vdash e'$$

In the first case, $\overline{\sigma\eta} \vdash e'$, the event e' is not performed on credit, hence $e' \notin \Gamma(\sigma')$ – contradiction. In the second case, by monotonicity of the function $\lambda X.\ X \cup \mathcal{R}^X$, we get $\overline{\sigma'} \cup \mathcal{R}^{\overline{\sigma'}} \Vdash e'$. If we can prove that

$\mathcal{R}^{\overline{\sigma'}} \subseteq \overline{\sigma'}$, we reach a contradiction because $\overline{\sigma'} \Vdash e'$ implies that the credit e' has been honoured, hence $e' \notin \Gamma(\sigma')$.

We are then left with proving $\mathcal{R}^{\overline{\sigma'}} \subseteq \overline{\sigma'}$. By contradiction, assume there exists $e_1 \in \mathcal{R}^{\overline{\sigma'}} \setminus \overline{\sigma'}$. By definition of $\mathcal{R}^{\overline{\sigma'}}$, there exist η, η' such that $\overline{\eta} = \overline{\sigma'}$, $e_1 \in \overline{\eta'}$, $\Gamma(\eta\eta') \subseteq \overline{\eta} = \overline{\sigma'}$ — and indeed $\overline{\eta'} \subseteq \mathcal{R}^{\overline{\sigma'}}$. Let e_0 be the first event in η' such that $e_0 \notin \overline{\sigma'}$ (which must exist because $e_1 \in \overline{\eta'}$). Then, $\eta\eta' = \eta\eta_0 e_0 \eta_1$ for some η_0, η_1. Clearly, $\overline{\eta\eta_0} \subseteq \overline{\sigma'}$. We have the following two cases:

- $\overline{\eta\eta_0} \vdash e_0$. In this case, we have $e_0 \in \mathcal{P}^{\overline{\sigma'}}$.
- $\overline{\eta\eta'} \Vdash e_0$. Since $\overline{\eta\eta'} \subseteq \overline{\sigma'} \cup \mathcal{R}^{\overline{\sigma'}}$, then by saturation $\overline{\sigma'} \cup \mathcal{R}^{\overline{\sigma'}} \Vdash e_0$. Hence we would have $e_0 \in \mathcal{P}^{\overline{\sigma'}}$.

In both cases we obtained $e_0 \in \mathcal{P}^{\overline{\sigma'}}$ but $e_0 \notin \overline{\sigma'}$. However, if $\pi(e_0) = \mathsf{A}$, then we would have that σ' is not fair respect to Σ_{A} – contradiction. If instead $\pi(e_0) = \mathsf{B} \neq \mathsf{A}$, then we would have $(\mathsf{B}, \sigma') \notin I$, contradicting our earlier assumption. Summing up, this concludes the proof of $\mathcal{R}^{\overline{\sigma'}} \subseteq \overline{\sigma'}$, hence the one for $P \subseteq P'$ as well.

We now prove that $I \supseteq I'$. Actually, we shall prove the contrapositive, i.e. whenever $(\mathsf{A}, \sigma) \notin I$, it must be $(\mathsf{A}, \sigma) \notin I'$. Let $(\mathsf{A}, \sigma) \notin I$. By definition of I, there must exist some $e \in \pi^{-1}(\mathsf{A})$ such that $e \in \mathcal{P}^{\overline{\sigma}}$. Let $i = |\overline{\sigma}|$. Then, for all $j \geq i$, $e \in \mathcal{P}^{\overline{\sigma_j}}$ (indeed, since $\sigma_i = \sigma$ we can only have $j = i$). By definition of P, this amounts to say that $(e, \sigma_j) \in P$. In conclusion, we have found an event $e \in \pi^{-1}(\mathsf{A})$ for which there exists some i such that, for all $j \geq i$, $(e, \sigma_j) \in P$. By definition of I', this proves that $(\mathsf{A}, \sigma) \notin I'$.

($\Rightarrow$) Assume that e is prudent for A in σ. We must prove that $e \in \mathcal{P}^{\overline{\sigma}}$. For all participants B, consider the greatest prudent strategy Σ^p_{B}. Clearly, we can pick a fair trace $\sigma' = \sigma\, e\, \nu$ such that ν conforms to *all* the strategies Σ_{B}. By fairness and by definition of innocence, all participants are innocent in σ'. We now prove that $\Gamma(\sigma') \subseteq \Gamma(\sigma)$. Let $\sigma' = \sigma\langle e_0 \cdots e_n \rangle$ (recall that E is finite). By contradiction, assume that for some e_i (say, of participant B), $e_i \in \Gamma(\sigma')$ but $e_i \notin \Gamma(\sigma)$. Since all events in $e\,\nu$ are prudent, then by Definition 2.12:

$$\exists k > |\sigma_i|.\ \Gamma(\sigma'_k) \cap \pi^{-1}(\mathsf{B}) \ \subseteq\ \Gamma(\sigma_i) \subseteq \overline{\sigma_i} \not\ni e_i$$

That is, each event taken on credit is eventually removed from the credits. Since once removed, an event can no longer appear in the credits, we reach a contradiction with $e_i \in \Gamma(\sigma')$. By $\Gamma(\sigma') \subseteq \Gamma(\sigma)$ and by the definition of $\mathcal{R}$, it follows that $\overline{e\nu} \subseteq \mathcal{R}^{\overline{\sigma}}$. Now there are two cases. If $\overline{\sigma} \vdash e$, then we trivially have the thesis. Otherwise, it must be the case that $\overline{\sigma'} \Vdash e$. Since $\overline{\sigma'} = \overline{\sigma e \nu} \subseteq \overline{\sigma} \cup \mathcal{R}^{\overline{\sigma}}$, by saturation we conclude that $\overline{\sigma} \cup \mathcal{R}^{\overline{\sigma}} \Vdash e$. Therefore, $e \in \mathcal{P}^{\overline{\sigma}}$. □

Lemma B.2. *For a conflict-free contract $\mathcal{C}$, the strategy:*

$$\Sigma^p_{\mathsf{A}} = \lambda\sigma.\, \{e \in \pi^{-1}(\mathsf{A}) \mid e \text{ is prudent in } \sigma\}$$

is prudent for A in $\mathcal{C}$. Furthermore, A is innocent in all fair plays conforming to Σ^p_{A}.

Proof. Let $\sigma = \langle e_0 \cdots e_n \rangle$ be a fair play where A does all her prudent events and all other participants are innocent. Clearly, also A is innocent in σ, hence by Lemma B.1, σ contains exactly the reachable events $\mathcal{R}^{\emptyset}$. By Lemma 4.5, for all $i < |\sigma|$, e_i is prudent in σ_i iff $e \in \mathcal{P}^{\overline{\sigma_i}}$, i.e. if either $\overline{\sigma_i} \vdash e_i$ or $\overline{\sigma_i} \cup \mathcal{R}^{\overline{\sigma_i}} \Vdash e_i$. In the first case, e_i does not augment the credits; in the second case, if e_i is taken on credit then the credit is eventually honoured, because $\overline{\sigma} = \mathcal{R}^{\emptyset} \supseteq \overline{\sigma_i} \cup \mathcal{R}^{\overline{\sigma_i}}$ (and so, $\overline{\sigma} \Vdash e_i$). Therefore, $\Gamma(\sigma) = \emptyset$, from which the thesis follows. □

Theorem 4.2. *Let $\Delta \sim \mathcal{E}$, and let Φ be a reachability payoff induced by φ. Then, A agrees on $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ iff $\{a \mid \Delta \vdash a\} \in \varphi(\mathsf{A})$.*

Proof. In [27] a bijection $[\cdot]_{\mathcal{R}}$ is defined from conflict-free CES into the Horn fragment of PCL. The encoding $[\cdot]_{\mathcal{R}}$ maps an enabling $\vdash$ into an $\rightarrow$-clause, and a circular enabling $\Vdash$ into an $\twoheadrightarrow$-clause, as follows:

$$\begin{aligned} [(X_i \triangleright e_i)_{i \in I}]_{\mathcal{R}} &= \{[X_i \triangleright e_i]_{\mathcal{R}} \mid i \in I\} \\ [X \triangleright e]_{\mathcal{R}} &= \big(\bigwedge X\big)\, [\triangleright]\, e \end{aligned} \qquad \text{where } [\triangleright] = \begin{cases} \rightarrow & \text{if } \triangleright = \vdash \\ \twoheadrightarrow & \text{if } \triangleright = \Vdash \end{cases}$$

Lemma 6.3 and Theorem 6.4 in [27] show that, for all $e \in E$:

$$e \in \mathcal{R}^{\emptyset} \iff [\mathcal{E}]_{\mathcal{R}} \vdash e \tag{12}$$

Roughly, this amounts to say that if $\Delta \sim \mathcal{E}$ then the reachable events of $\mathcal{E}$ coincide with the provable atoms in Δ. We now exploit (12) to prove the statement of Theorem 4.2.

For the ($\Rightarrow$) direction, assume that A agrees on $\mathcal{C}$. By (12), $\{a \mid \Delta \vdash a\} = \mathcal{R}^{\emptyset}$. Let σ be a fair play conforming to the winning strategy of A, and conforming the the prudent strategies Σ^p_{B} of the other participants B. Since A wins in σ, then $\sigma \in \Phi\mathsf{A}$. Now, Φ is a reachability payoff induced by φ, hence $\overline{\sigma} \in \varphi(\mathsf{A})$. Since $\mathcal{E}$ is conflict-free, and since all the participants are innocent in σ (Lemma B.2), then by Lemma B.1 it follows that $\overline{\sigma} = \mathcal{R}^{\emptyset}$, from which the thesis $\{a \mid \Delta \vdash a\} \in \varphi(\mathsf{A})$ follows.

For the ($\Leftarrow$) direction, the proof is specular to the above. □

For conflict-free CES, we can inductively characterize the reachable events and the prudent events (with past C) as the sets $\hat{\mathcal{R}}$ and $\hat{\mathcal{U}}^C$, respectively. Lemmas B.4 and B.5 below provide some structural properties of $\hat{\mathcal{R}}$ and $\hat{\mathcal{U}}^C$, respectively, to be exploited in the subsequent proof of Lemma B.8.

Definition B.3. *For a* CES $\mathcal{E}$ *and for all* $C, X \subseteq E$*, we define the sets* $\hat{\mathcal{R}}(X)$ *and* $\hat{\mathcal{U}}^C(X)$ *as follows:*

$$\frac{e \in X}{e \in \hat{\mathcal{R}}(X)}\ (\in_{\hat{\mathcal{R}}}) \qquad \frac{\hat{\mathcal{R}}(X) \vdash e}{e \in \hat{\mathcal{R}}(X)}\ (\vdash_{\hat{\mathcal{R}}}) \qquad \frac{\hat{\mathcal{R}}(X \cup \{e\}) \Vdash e}{e \in \hat{\mathcal{R}}(X)}\ (\Vdash_{\hat{\mathcal{R}}})$$

$$\frac{e \in C}{e \in \hat{\mathcal{U}}^C(X)}\ (\in_{\hat{\mathcal{U}}}) \qquad \frac{C \vdash e}{e \in \hat{\mathcal{U}}^C(X)}\ (\vdash_{\hat{\mathcal{U}}}) \qquad \frac{\hat{\mathcal{R}}(C \cup X) \Vdash e}{e \in \hat{\mathcal{U}}^C(X)}\ (\Vdash_{\hat{\mathcal{U}}})$$

Lemma B.4. *For a conflict-free* CES $\mathcal{E}$*, for all* $X, Y \subseteq E$*, and for all* $Z \subseteq_{fin} E$*:*

(a) $X \subseteq \hat{\mathcal{R}}(X)$

(b) $X \subseteq Y \implies \hat{\mathcal{R}}(X) \subseteq \hat{\mathcal{R}}(Y)$.

(c) $\hat{\mathcal{R}}(\hat{\mathcal{R}}(X)) = \hat{\mathcal{R}}(X)$

(d) $Y \subseteq \hat{\mathcal{R}}(X) \implies \hat{\mathcal{R}}(X \cup Y) = \hat{\mathcal{R}}(X)$

(e) $\hat{\mathcal{R}}(X \cup Z) \Vdash Z \implies Z \subseteq \hat{\mathcal{R}}(X)$

(f) $\hat{\mathcal{R}}(X \cup Z) \Vdash Z \implies \hat{\mathcal{R}}(X \cup Z) = \hat{\mathcal{R}}(X)$

Proof. For items (a), (b), (c), see Lemma A.2 in [27]. For item (d), see Lemma A.3 in [27]. For item (e), see Lemma A.4 in [27]. For item (f), by Lemma B.4(e) we have $Z \subseteq \hat{\mathcal{R}}(X)$. The thesis follows by Lemma B.4(d). □

Lemma B.5. *For a conflict-free* CES $\mathcal{E}$*, and for all* $C, C', X, Y \subseteq E$*:*

(a) $C \subseteq C' \wedge X \subseteq Y \implies \hat{\mathcal{U}}^C(X) \subseteq \hat{\mathcal{U}}^{C'}(Y)$

(b) $Y \subseteq \hat{\mathcal{R}}(X) \implies \hat{\mathcal{U}}^C(X \cup Y) \subseteq \hat{\mathcal{U}}^C(X)$

(c) $\hat{\mathcal{U}}^C(X) \subseteq \hat{\mathcal{R}}(C \cup X)$

Proof. All the items are straightforward by Definition B.3. □

Notation B.6. *Hereafter, when* $\Delta \sim \mathcal{E}$ *we shall write* $[\mathcal{E}]_{\mathcal{U}}$ *for* $[\Delta]_{\mathcal{U}}$.

Lemma B.7. $[\mathcal{E}]_{\mathcal{U}}, \Phi \vdash \varphi \implies \overline{\varphi}^{!} \subseteq \overline{\Phi}^{!}$

Proof. Straightforward induction on the depth of the proof of $[\mathcal{E}]_{\mathcal{U}}, \Phi \vdash \varphi$. □

Lemma B.8. *For all $C \subseteq E$ and $e \in E$:*

(a) $e \in \hat{\mathcal{R}}_{\mathcal{E}} \iff [\mathcal{E}]_{\mathcal{U}} \vdash Re$

(b) $e \in \hat{\mathcal{U}}^{C}_{\mathcal{E}} \iff [\mathcal{E}]_{\mathcal{U}}, !C \vdash Ue$

Proof. Note that, after Theorem 3.2, we can use for the entailment relation $\vdash$ the Gentzen rules for PCL. For the ($\Leftarrow$) direction, we shall first prove the following statement. For all sets of atoms Γ, and for all conjunctions of atoms φ:

$$[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash \varphi \implies \begin{cases} \overline{\varphi}^{R} \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR}) & \text{(13a)} \\ \overline{\varphi}^{U} \subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^{U} & \text{(13b)} \end{cases}$$

Since the Gentzen proof system of PCL enjoys cut elimination [15], we can consider a proof tree π of $[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash \varphi$ without occurrences of the (Cut) rule. The RHS of each sequent in π is a conjunction of atoms, and so π only contains occurrences of the rules (Id), ($\wedge$L1), ($\wedge$L2), ($\wedge$R), ($\to$L), (Fix). We prove (13a) and (13b) by induction on the depth of π.

The base case concerns the axiom (Id), which gives $[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash \varphi$ whenever $\varphi \in \Gamma$. For (13a), we have $\overline{\varphi}^{R} \subseteq \overline{\Gamma}^{R} \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{R}) \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR})$. For (13b), we have $\overline{\varphi}^{U} \subseteq \overline{\Gamma}^{U}$.

For the inductive case, we analyse the last rule used in π. There are the following exhaustive cases:

- ($\wedge$L1) and ($\wedge$L2). Straightforward by the induction hypothesis.
- ($\wedge$R). For some conjunctions of atoms p and q such that $\varphi = p \wedge q$:

$$\frac{[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash p \qquad [\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash q}{[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash p \wedge q} \ (\wedge\text{R})$$

  By applying the induction hypotheses of (13a) and (13b) on the two premises:

$$\begin{aligned} \overline{\varphi}^{R} &= \overline{(p \wedge q)}^{R} = \overline{p}^{R} \cup \overline{q}^{R} \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR}) \\ \overline{\varphi}^{U} &= \overline{(p \wedge q)}^{U} = \overline{p}^{U} \cup \overline{q}^{U} \subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^{U} \end{aligned}$$

- ($\to$L). We have $p \to q \in [\mathcal{E}]_{\mathcal{U}}$ for some conjunctions of atoms p and q, and:

$$\frac{[\mathcal{E}]_{\mathcal{U}}, \Gamma, p \to q \vdash p \qquad [\mathcal{E}]_{\mathcal{U}}, \Gamma, q \vdash \varphi}{[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash \varphi} \ (\to\text{L})$$

  According to Definition 3.16, the formula $p \to q \in [\mathcal{E}]_{\mathcal{U}}$ must have one of following forms:

  – $!e \to Ue$. We have that $\overline{q}^{U} = \{e\}$, while $\overline{q}^{!R} = \emptyset$. By applying the induction hypothesis to the rightmost premise of the rule, we obtain:

$$\begin{aligned} \overline{\varphi}^{R} &\subseteq \hat{\mathcal{R}}(\overline{\Gamma, q}^{!UR}) = \hat{\mathcal{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \\ \overline{\varphi}^{U} &\subseteq \hat{\mathcal{U}}^{\overline{\Gamma, q}^{!}}(\overline{\Gamma, q}^{UR}) \cup \overline{\Gamma, q}^{U} = \hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^{U} \cup \{e\} \end{aligned}$$

    By the leftmost premise of the rule we have that $[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash !e$. Then, by Lemma B.7 it must be $e \in \overline{\Gamma}^{!}$.

    For (13a), we have $\overline{\Gamma}^{!UR} \cup \{e\} = \overline{\Gamma}^{!UR}$, from which the thesis follows.

    For (13b), by Definition B.3 we have $\hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR} \cup \{e\}) = \hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR})$ and $e \in \hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(X)$ for all X, from which the thesis follows.

– $Ue \to Re$. We have that $\overline{q}^R = \{e\}$, while $\overline{q}^{!U} = \emptyset$. By applying the induction hypothesis to both premises of the rule, we obtain:

$$e \in \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^U \tag{14}$$

$$\overline{\varphi}^R \subseteq \hat{\mathcal{R}}(\overline{\Gamma, q}^{!UR}) = \hat{\mathcal{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \tag{15}$$

$$\overline{\varphi}^U \subseteq \hat{\mathcal{U}}^{\overline{\Gamma,q}^!}(\overline{\Gamma, q}^{UR}) \cup \overline{\Gamma, q}^U = \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^U \tag{16}$$

From (14), Lemma B.4 gives that $e \in \hat{\mathcal{R}}(\overline{\Gamma}^{!UR}) \cup \overline{\Gamma}^U = \hat{\mathcal{R}}(\overline{\Gamma}^{!UR})$. By applying Lemma B.4(b) to (15), we have $\overline{\varphi}^R \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR} \cup \hat{\mathcal{R}}(\overline{\Gamma}^{!UR}))$. Lemma B.4(c) allows then to obtain the thesis of (13a), i.e. $\overline{\varphi}^R \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR})$.
For (13b), we have that:

$$\begin{aligned}
\overline{\varphi}^U &\subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^U && \text{by (16)} \\
&= \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{!UR} \cup \{e\}) \cup \overline{\Gamma}^U && \text{by Definition B.3} \\
&\subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{!UR}) \cup \overline{\Gamma}^U && \text{by Lemma B.5(b)} \\
&= \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^U && \text{by Definition B.3}
\end{aligned}$$

– $RX \to Re$. This has been generated because of an enabling $X \vdash e$ in $\mathcal{E}$. By applying the induction hypothesis to both premises of the rule:

$$X \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR}) \tag{17}$$

$$\overline{\varphi}^R \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \tag{18}$$

$$\overline{\varphi}^U \subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^U \tag{19}$$

For (13a), $X \vdash e$ and (17) imply that $e \in \hat{\mathcal{R}}(\overline{\Gamma}^{!UR})$. Then, we can apply Lemma B.4(c) to (18) and obtain the thesis $\overline{\varphi}^R \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR})$.
For (13b), we have that:

$$\begin{aligned}
\overline{\varphi}^U &\subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^U && \text{by (19)} \\
&= \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{!UR} \cup \{e\}) \cup \overline{\Gamma}^U && \text{by Definition B.3} \\
&\subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{!UR}) \cup \overline{\Gamma}^U && \text{by Lemma B.5(b)} \\
&= \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^U && \text{by Definition B.3}
\end{aligned}$$

– $!X \to Ue$. This has been generated because of an enabling $X \vdash e$ in $\mathcal{E}$. By applying the induction hypothesis to the rightmost premise of the rule:

$$\begin{aligned}
\overline{\varphi}^R &\subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \\
\overline{\varphi}^U &\subseteq \hat{\mathcal{U}}^{\overline{\Gamma}^!}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^U \cup \{e\}
\end{aligned}$$

By the leftmost premise of the rule we have that $[\mathcal{E}]_{\mathcal{U}}, \Gamma \vdash !X$, and so by Lemma B.7 it must be $X \subseteq \overline{\Gamma}^!$. Therefore, $\overline{\Gamma}^! \vdash e$, from which we conclude that $e \in \hat{\mathcal{R}}(\overline{\Gamma}^!) \subseteq \hat{\mathcal{R}}(\overline{\Gamma}^{!UR})$. Lemma B.4(c) gives the thesis for (13a).

For (13b), from $\overline{\Gamma}^! \vdash e$ it follows that $e \in \hat{\mathcal{U}}^{\overline{\Gamma}^!}(X)$, for all X. The thesis follows from Lemma B.5(c) and Lemma B.5(b).

- (Fix). We have that $p \twoheadrightarrow q \in [\mathcal{E}]_{\mathcal{U}}$ for some conjunctions of atoms p and q, and:

$$\frac{[\mathcal{E}]_{\mathcal{U}},\, \Gamma,\, p \twoheadrightarrow q,\, \varphi \vdash p \qquad [\mathcal{E}]_{\mathcal{U}},\, \Gamma,\, q \vdash \varphi}{[\mathcal{E}]_{\mathcal{U}},\, \Gamma \vdash \varphi}\ (\textsc{Fix})$$

By Definition 3.16, the formula $p \twoheadrightarrow q \in [\mathcal{E}]_{\mathcal{U}}$ must have been obtained as the encoding of a circular enabling $X \Vdash e$ in $\mathcal{E}$, which gives $p = RX$ and $q = Ue$.

By applying the induction hypothesis to both premises of rule (Fix):

$$X \;\subseteq\; \hat{\mathfrak{R}}(\overline{\Gamma, \varphi}^{!UR}) \;=\; \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \overline{\varphi}^{!UR}) \tag{20}$$

$$\overline{\varphi}^{R} \;\subseteq\; \hat{\mathfrak{R}}(\overline{\Gamma, q}^{!UR}) \;\subseteq\; \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \tag{21}$$

$$\overline{\varphi}^{U} \;\subseteq\; \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^{U} \cup \{e\} \tag{22}$$

We have that:

$$\begin{aligned}
X &\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \overline{\varphi}^{!UR}) && \text{by (20)}\\
&\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \overline{\varphi}^{UR}) && \text{by Lemma B.7}\\
&\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \overline{\varphi}^{U} \cup \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\})) && \text{by (21)}\\
&\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\} \cup \overline{\varphi}^{U} \cup \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\})) && \text{by Lemma B.4(b)}\\
&\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \overline{\varphi}^{U} \cup \{e\}) && \text{by Lemma B.4(c)}\\
&\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^{U} \cup \{e\}) && \text{by (22)}\\
&= \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR} \cup \{e\})) && \text{by Lemma B.4(f)}\\
&\subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\})) && \text{by Lemma B.5(c)}\\
&= \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR})) && \text{by Lemma B.4(f)}\\
&= \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR}) && \text{by Lemma B.4(c)}
\end{aligned}$$

For (13a), since $X \subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \Vdash e$, by Lemma B.4(f) we obtain the thesis:

$$\overline{\varphi}^{R} \;\subseteq\; \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR} \cup \{e\}) \;=\; \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR})$$

For (13b), since $X \subseteq \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR}) \Vdash e$, then $e \in \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR}) = \hat{\mathfrak{R}}(\overline{\Gamma}^{!} \cup \overline{\Gamma}^{UR})$. By Definition B.3 it follows that $e \in \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR})$. Thus:

$$\begin{aligned}
\overline{\varphi}^{U} &\subseteq \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR} \cup \{e\}) \cup \overline{\Gamma}^{U} \cup \{e\} && \text{by (22)}\\
&= \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{!UR} \cup \{e\}) \cup \overline{\Gamma}^{U} \cup \{e\} && \text{by Definition B.3}\\
&\subseteq \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{!UR}) \cup \overline{\Gamma}^{U} \cup \{e\} && \text{by Lemma B.5(b)}\\
&= \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^{U} \cup \{e\} && \text{by Definition B.3}\\
&= \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^{U} && \text{since } e \in \hat{\mathfrak{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR}).
\end{aligned}$$

We now prove that (13a) and (13b) imply items a and b of Lemma B.8, respectively.
For item a, assume that $[\mathcal{E}]_{\mathcal{U}} \vdash Re$. Let $\Gamma = \emptyset$ and $\varphi = Re$. By (13a) we obtain:

$$\{e\} \;=\; \overline{\varphi}^{R} \;\subseteq\; \hat{\mathfrak{R}}(\overline{\Gamma}^{!UR}) \;=\; \hat{\mathfrak{R}}(\emptyset) \;=\; \hat{\mathfrak{R}}_{\mathcal{E}}$$

For item b, assume that $[\mathcal{E}]_{\mathcal{U}}, !C \vdash Ue$. Let $\Gamma = !C$, and let $\varphi = Ue$. Then, $\overline{\Gamma}^{!} = C$, $\overline{\Gamma}^{UR} = \emptyset$, and $\overline{\varphi}^{U} = \{e\}$. By (13b) we obtain:

$$\{e\} \;=\; \overline{\varphi}^{U} \;\subseteq\; \hat{\mathcal{U}}^{\overline{\Gamma}^{!}}(\overline{\Gamma}^{UR}) \cup \overline{\Gamma}^{U} \;=\; \hat{\mathcal{U}}^{C}(\emptyset) \;=\; \hat{\mathcal{U}}^{C}$$

For the ($\Rightarrow$) direction of item (a), we prove the following stronger statement. For all X, if $e \in \hat{\mathfrak{R}}(X)$ then $[\mathcal{E}]_{\mathcal{U}}, RX \vdash Re$. Assume that $e \in \hat{\mathfrak{R}}(X)$. We proceed by induction on the derivation of $e \in \hat{\mathfrak{R}}(X)$. According to the last rule used in the derivation, there are the following cases:

- ($\in_{\hat{\mathfrak{R}}}$). We have $e \in X$, from which the thesis follows trivially.
- ($\vdash_{\hat{\mathfrak{R}}}$). We have $\hat{\mathfrak{R}}(X) \vdash e$. Let $C_0 \subseteq \hat{\mathfrak{R}}(X)$ be a minimal set such that $C_0 \vdash e$. By the induction hypothesis, $[\mathcal{E}]_{\mathcal{U}}, RX \vdash RC_0$. Also, by Definition 3.16, $RC_0 \to Re \in [\mathcal{E}]_{\mathcal{U}}$. Therefore, by rule ($\to$L):

$$\frac{[\mathcal{E}]_{\mathcal{U}},\, RX,\, RC_0 \to Re \vdash RC_0 \qquad [\mathcal{E}]_{\mathcal{U}},\, RX,\, Re \vdash Re}{[\mathcal{E}]_{\mathcal{U}},\, RX \vdash Re}$$

- ($\Vdash_{\hat{\mathfrak{R}}}$). We have $\hat{\mathfrak{R}}(X \cup \{e\}) \Vdash e$. Let $C_0 \subseteq \hat{\mathfrak{R}}(X \cup \{e\})$ be a minimal set such that $C_0 \Vdash e$. By the induction hypothesis, $[\mathcal{E}]_{\mathcal{U}}, RX, Re \vdash RC_0$. Also, by Definition 3.16, $RC_0 \twoheadrightarrow Ue \in [\mathcal{E}]_{\mathcal{U}}$. Therefore, by rule (Fix):

$$\frac{[\mathcal{E}]_{\mathcal{U}},\, RX,\, RC_0 \twoheadrightarrow Ue,\, Re \vdash RC_0 \qquad [\mathcal{E}]_{\mathcal{U}},\, RX,\, Ue \vdash Re}{[\mathcal{E}]_{\mathcal{U}},\, RX \vdash Re}$$

  where the second premise has been obtained because $Ue \to Re \in [\mathcal{E}]_{\mathcal{U}}$.

For the ($\Rightarrow$) direction of item (b), assume that $e \in \hat{\mathcal{U}}^{C}$. We proceed by cases on the rule used in the derivation.

- ($\in_{\hat{\mathcal{U}}}$). We have that $e \in C$. Therefore, $[\mathcal{E}]_{\mathcal{U}}, !C \vdash !e$, and since $!e \to Ue \in [\mathcal{E}]_{\mathcal{U}}$ we obtain the thesis.
- ($\vdash_{\hat{\mathcal{U}}}$). By the rule premise, it must be $C \vdash e$. Let $C_0 \subseteq C$ be a minimal set such that $C_0 \vdash e$. Then, $\big((RC_0 \to Re) \wedge (!C_0 \to Ue)\big) \in [\mathcal{E}]_{\mathcal{U}}$. Since $C_0 \subseteq C$, then $!C_0 \to Ue$ implies that $!C \to Ue$. Therefore, $[\mathcal{E}]_{\mathcal{U}}, !C \vdash Ue$.
- ($\Vdash_{\hat{\mathcal{U}}}$). By the rule premise, it must be $C \cup \mathcal{R}^{C} \Vdash e$. Let $C_0 \subseteq C \cup \mathcal{R}^{C}$ be a minimal set such that $C_0 \Vdash e$. By Definition 3.16, $RC_0 \twoheadrightarrow Ue \in [\mathcal{E}]_{\mathcal{U}}$. Since the encoding $[\mathcal{E}]_{\mathcal{U}}$ comprises $!e \to Ue$ and $Ue \to Re$ for all e, then $[\mathcal{E}]_{\mathcal{U}}, !C \vdash RC$. By Item a, $[\mathcal{E}]_{\mathcal{U}}, !C \vdash R(\mathcal{R}^{C})$. Thus, $[\mathcal{E}]_{\mathcal{U}}, !C \vdash RC_0$. Then, we can weaken $RC_0 \twoheadrightarrow Ue$ to $RC_0 \to Ue$, and use rule ($\to$L) to deduce $[\mathcal{E}]_{\mathcal{U}}, !C \vdash Ue$.

□

Lemma 4.7. *Let $\Delta \sim \mathcal{E}$. Then, for all $X \subseteq E$, $\mathcal{P}^{X}_{\mathcal{E}} = \mathcal{U}^{X}_{\Delta}$.*

Proof. We have that:

$$\begin{array}{lll}
e \in \mathcal{P}^{X}_{\mathcal{E}} & \iff e \in \hat{\mathcal{U}}^{X}_{\mathcal{E}} \setminus X & \text{by Definition B.3} \\
& \iff [\mathcal{E}]_{\mathcal{U}}, !X \vdash Ue \;\wedge\; e \notin X & \text{by Lemma B.8(b)} \\
& \iff [\Delta]_{\mathcal{U}}, !X \vdash Ue \;\wedge\; e \notin X & \text{as } \Delta \sim \mathcal{E} \\
& \iff e \in \mathcal{U}^{X}_{\Delta} \;\wedge\; e \notin X & \text{by Theorem 3.21} \\
& \iff e \in \mathcal{U}^{X}_{\Delta} & \text{since } \mathcal{U}^{X}_{\Delta} \cap X = \emptyset
\end{array}$$

□

Theorem 4.11. *Let $\Delta \sim \mathcal{E}$, and let the strategy Σ_{A} be defined as:*

$$\Sigma_{\mathsf{A}}(\sigma) \;=\; \mathcal{U}_{\Delta}^{\overline{\sigma}} \cap \pi^{-1}(\mathsf{A})$$

Then, Σ_{A} is a prudent strategy for A in $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$. Moreover, if Φ is a reachability payoff and $\mathcal{C}$ admits an agreement, then Σ_{A} is winning for A.

Proof. By Lemma 4.7, $\mathcal{U}_{\Delta}^{\overline{\sigma}} = \mathcal{P}_{\mathcal{E}}^{\overline{\sigma}}$. By Lemma 4.5, $\mathcal{P}_{\mathcal{E}}^{\overline{\sigma}}$ contains all and only the prudent events in σ. Thus, by Lemma B.2, Σ_{A} is the maximal prudent strategy for A. For the second part, assume that $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ admits an agreement, and that Φ is a reachability payoff induced by φ. Let σ' be a play where all the participants win: then, $\overline{\sigma'} \in \varphi(\mathsf{A})$, and A is credit-free in σ'. By Lemma B.1, $\overline{\sigma'} = \mathcal{R}^{\emptyset}$. Now, let σ be a fair play conforming to Σ_{A}. If some $\mathsf{B} \neq \mathsf{A}$ is culpable, then A wins. Otherwise, by Lemma B.1, $\overline{\sigma} = \mathcal{R}^{\emptyset} = \overline{\sigma'} \in \varphi(\mathsf{A})$, and by Definition 2.12 A is credit-free. Then, we conclude that A wins in σ. □