Contract agreements via 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 and COSBI, Italy

We relate two contract models: one based on event structures and game theory, and the other one based on logic. In particular, we show that the notions of agreement and winning strategies in the game-theoretic model are related to that of provability in the logical model.

1 Introduction

Contracts are gaining an increasing relevance in the design and implementation of concurrent and distributed systems. This is witnessed by the proliferation of proposals of models and standards for contracts appeared in the literature in the last few years. For instance, *choreography languages* like WS-CDL [21], BPEL4Chor [16] and Scribble [19] can be used to specify the overall interaction protocol of a set of Web services. By projecting a choreography on each of the participants, we obtain the specification of the behaviour expected from each single service involved in the application. These projections can be interpreted as contracts: if the actual implementation of each Web service respects its contract, then the overall application is guaranteed to behave correctly; otherwise, the service violating its contract may be responsible (and punishable) for the global failure. On a more theoretical side, formal models for contracts have been devised by adapting and extending models of concurrent systems, such as Petri nets [1], event structures [18, 8], process algebras [12, 13, 14, 15, 20], timed automata [22, 24], and by extending various logics, such as modal [2], intuitionistic [3, 11], linear [3], and deontic [23, 17] logics (just to cite a few recent approaches).

A main motivation for using contracts resides in the fact that large distributed applications are often constructed by dynamically discovering and composing services published by different organizations. The larger an application is, the great the probability that some of its components deviates from the expected behaviour (either because of unintentional bugs, or maliciousness of a competing organization). Hence, it becomes crucial to protect oneself from other participants' misbehaviour. Standard enforcement mechanisms do not apply, because of the total lack of control on code run by mutually untrusted, distributed participants. Instead, contracts may offer protection by legally binding the participants in a service composition to either behave as prescribed, or otherwise be blamed for a contract breach [4].

In this methodology, contracts are the pillars which support the reliability of distributed applications, hence the choice of the actual contract model to be used is critical. However, the ecosystem of contract models proposed in the literature is wide and heterogeneous, and the actual properties and the relations among different models are not clearly established. In particular, there is a gap between the two main paradigms for modelling contracts, i.e. the one which interprets them as interactive multi-agent systems, and the one where contracts are rendered as formulae of suitable logics. To contribute towards reducing this gap, in this paper we consider two recent models for contracts — one based on game-theoretic notions and the other one on logic — and we formally relate them. More precisely, we show that a cor-

To appear in EPTCS.

respondence exists between the fundamental notions in the first model (namely, *agreements* and *winning strategies*) and provability in the logic-based model.

In the first model [9], the behaviour of a set of interacting participants is specified as a concurrent multi-player game. The plays of the game are traces of an event structure (ES) which models the causal relations among the actions of the participants. Intuitively, an enabling $X \vdash e$ in an ES models the fact that the action e becomes an *obligation* after all the actions in X have been performed. A participant A wins in a play when (i) her *payoff* (defined by a given function Φ) is positive in that play, or (ii) some participant (but not A) can be blamed for a contract violation. Indeed, if some $\mathsf{B} \neq \mathsf{A}$ has violated his contract, an external judge may eventually provide A with the prescribed compensation (and B with the respective punishment).

Two key notions in this model are that of *agreement* and *protection*. Intuitively, given a set of contracts, the agreement property guarantees that each involved participant has a *winning* strategy. Instead, protection is the property of a single contract $\mathcal{C}$ of A ensuring that, whenever $\mathcal{C}$ is composed with any other contract (possibly that of an adversary), A has a *non-losing* strategy. In [9] it is shown that agreement and protection cannot coexist in a broad class of contracts where the obligations are modelled as Winskel's ES [26]. Roughly, to be protected one should wait until the conditions X in some enabling $X \vdash e$ are satisfied before doing the event e. If all participants adhere to this principle, agreement is not possible. To reconcile agreements with protection, an extension of Winskel's ES has been proposed, which allows for decoupling a conditional promise (e.g., doing e in change of X) from the temporal order in which events are performed. In an ES *with circular causality* (CES for short), an enabling $b \Vdash a$ means that "A will do a if B *promises* to do b". This contract protects A, and when composed with the contract $a \Vdash b$ of B, it admits an agreement. More in general, in [9] a technique is proposed which, given the participants payoffs, synthesises a set of contracts which guarantee both agreement and protection.

The second model we consider is an extension of intuitionistic propositional logic (IPC), called Propositional Contract Logic (PCL [11]). PCL features a "contractual" form of implication, denoted by $\twoheadrightarrow$. The intuition is that a formula $p \twoheadrightarrow q$ entails q not only when p is provable, like standard intuitionistic implication, 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, $(p \twoheadrightarrow q) \wedge (q \twoheadrightarrow p) \to p \wedge q$ is a theorem of PCL. The logic PCL is decidable [11].

A first observation about these two models is that they both allow for a form of "circular" assume-guarantee reasoning. Consider, for example, a participant A which promises to do a provided that she receives b in exchange, and a participant B which, dually, promises to do b in exchange of a. In the game-theoretic model, these obligations are represented by a CES with enablings $b \Vdash a$ and $a \Vdash b$. Given the intended payoff functions, this contract admits an agreement. The winning strategies of A and B prescribe both participants to do their events (without waiting for the other to take the first step), so leading to a *configuration* $\{a, b\}$ of the CES. In the logical model, the scenario above is represented by the PCL formula $(b \twoheadrightarrow a) \wedge (a \twoheadrightarrow b)$. As noted above, this formula entails both a and b in the proof system of PCL. Hence, a connection seems to exist between the agreement property in the game-theoretic model and provability in PCL.

A main contribution of this paper is to formalise this connection. More precisely, Theorem 4.5 shows that agreement in conflict-free contracts corresponds to provability in Horn PCL theories. This correspondence has an important consequence, since it provides us with a polynomial algorithm for provability in Horn PCL (in contrast with the fact that provability in *full* PCL is PSPACE-complete, as well as in IPC and in its implicational fragment [25]). We illustrate this point with the help of some examples (Ex. 4.1 and 4.2) where we show that apparently hard questions in PCL admit an easy answer

when passing to the realm of contracts.

We deepen the above-mentioned correspondence by relating winning strategies for the game-theoretic contracts with proofs in PCL. The idea is that a proof in the logic induces an ordering among the atoms. For instance, to use the elimination rule of $\to$ in a proof of $\Delta, a \to b \vdash b$, one must first construct a proof of a (similarly to the ordering imposed by an enabling $a \vdash b$), whereas in a proof of $\Delta, a \twoheadrightarrow b \vdash b$ the proofs of a and b can be interleaved (i.e. a can be proved after b, similarly to the fact that $a \Vdash b$ allows a to be done after b). We introduce in Section 3 the notion of *proof traces*, that represent the sequences of atoms respecting the order imposed by proofs in PCL. Theorem 4.9 states that proof traces correspond, in the contracts realm, to the plays where all participants are innocent. Since these plays can be constructed with a polynomial algorithm, this result is significant, because it allows for performing a non-trivial task in Horn PCL (i.e., constructing proof traces), through an easier one in contracts. Finally, Theorem 4.11 establishes that, whenever a contract admits an agreement, proof traces can be projected to winning strategies for all participants.

Because of space constraints, the proofs of our results are available in [5].

2 Background

2.1 Contracts

We briefly review the theory of contracts introduced in [9]. A contract is a concurrent system featuring *obligations* (what I must do in a given state) and *objectives* (what I wish to obtain in a given state).

Obligations are modelled as event structures with circular causality (CES). A comprehensive account of CES is in [7]; here we shall only recall the needed definitions. Assume 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 $\pi : E \to \mathcal{A}$. We denote with $\# \subseteq E \times E$ a *conflict* relation between events, namely if $a\#b$ then a and b cannot occur in the same computation. For a set $X \subseteq E$, the predicate $CF(X)$ is true iff X is *conflict-free*, i.e. $\forall e, e' \in X : \neg(e\#e')$. We denote with Con the set $\{X \subseteq_{fin} E \mid CF(X)\}$.

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;*
- $\vdash \subseteq Con \times E$ *is the* enabling *relation;*
- $\Vdash \subseteq Con \times E$ *is the* circular enabling *relation.*

The relations $\vdash$ *and* $\Vdash$ *are* saturated*, i.e.* $\forall X \subseteq Y \subseteq_{fin} E.\ X \circ e \wedge CF(Y) \implies Y \circ e$*, for* $\circ \in \{\vdash, \Vdash\}$.

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: e is an obligation if it is a *prudent* event (see Def. 2.5). Very roughly, e is prudent when one can perform it "on credit" and be guaranteed that, in all possible executions of the contract, either the credit will be honoured, or the debtor will be culpable of a contract violation. For instance, in the contract with enablings $b \Vdash a$ and $a \vdash b$, the first 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

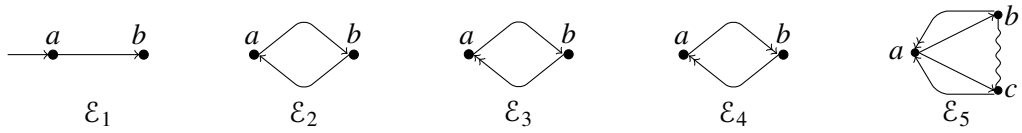


Figure 1: Graphical representation of CES. An hyperedge from a set of nodes X to e denotes an enabling $X \circ e$, where $\circ = \vdash$ if the edge has a single arrow, and $\circ = \Vdash$ if it has a double arrow. A conflict $a\#b$ is represented by a wavy line between a and b.

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).

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 $\Phi : \mathcal{A} \to \wp(E^\infty)$ associates each participant with a set of traces.*

We interpret a contract as a nonzero-sum concurrent multi-player game. The game involves the players in $\mathcal{A}$ concurrently performing actions in order to reach their objectives. A *play* of a contract $\mathcal{C}$ is a conflict-free sequence $\sigma \in E^\infty$ without repetitions. For $\sigma = \langle e_0\, e_1 \cdots \rangle \in E^\infty$, we write $\overline{\sigma}$ for the set of events in σ; 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 $\langle e_0 \cdots e_n\, e \rangle$. The empty sequence is denoted by ε.

Each play $\sigma = \langle e_0 \cdots e_i \cdots \rangle$ uniquely identifies a computation in the CES $\mathcal{E}$. This computation has the form $(\emptyset,\emptyset) \xrightarrow{e_0} (\overline{\sigma_1}, \Gamma(\sigma_1)) \cdots \xrightarrow{e_i} (\overline{\sigma_{i+1}}, \Gamma(\sigma_{i+1})) \cdots$. 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 $\Gamma(\eta) = \{e_i \in \overline{\eta} \mid \overline{\eta_i} \not\vdash e_i \wedge \overline{\eta} \Vdash e_i\}$. 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 2.3. *Consider the* CES *in Fig. 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).

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 play is *fair* w.r.t. a strategy Σ when there are no events in σ which are perpetually enabled by Σ.

Definition 2.4 (Fair play)**.** *A play $\sigma = \langle e_0\, e_1 \cdots \rangle$ is* fair *w.r.t. strategy Σ iff:*

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

Before setting up the crucial notion of prudent events, we provide some underlying intuitions. The definition of prudent strategies and of innocent participants is mutually coinductive. A participant A is considered *innocent* in a play σ when she has done all her prudent events in σ (otherwise A is *culpable*). Hence, if a strategy tells A to do all her prudent events, then in all *fair* plays these events must either become imprudent, or be fired. Given a finite play σ of past events, an event e is said *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, conform 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. Notice that we neglect those *unfair* plays where an action permanently enabled is not eventually performed. Indeed, an unfair scheduler could perpetually prevent an honest participant from performing a promised action.

Definition 2.5 (Prudence)**.** *A strategy Σ for* A *with past σ is* prudent *if, for all fair plays σ' extending σ, conform 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:*

$$\forall e \in \pi^{-1}(\mathsf{A}).\ \forall i \geq 0.\ \exists j \geq i.\ e \text{ is imprudent in } \sigma_j$$

Notice that the empty strategy is trivially prudent.

Example 2.6. *Consider the obligations modelled by the five* CES *in Fig. 1, where $\pi(a) = \mathsf{A}$ 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 $\langle c \rangle$.*

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

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

where A *is* credit-free *in σ iff:* $\forall e \in \pi^{-1}(\mathsf{A}).\ \forall i \geq 0.\ \exists j \geq i.\ e \notin \Gamma(\sigma_j)$.

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 disposses 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 conform to Σ.

Definition 2.8 (**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 2.9. *Consider the contracts* $\mathcal{C}_i$ *where the obligations are specified by* $\mathcal{E}_i$ *in Fig. 2.6, 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 conform 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 Ex. 2.3), 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 if they cannot reach their goals by doing nothing. If* A *does a, then* B *can b can choose to do c. This makes* B *innocent (and winning), but then* A *loses, because not credit-free in* $\langle ac \rangle$.

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

Figure 2: Sequent calculus for PCL (rules for $\twoheadrightarrow$; the full set of rules is in [5]).

$$\frac{\Delta \vdash q}{\Delta \vdash p \twoheadrightarrow q}\ (\twoheadrightarrow\text{I1}) \qquad \frac{\Delta \vdash p' \twoheadrightarrow q' \quad \begin{array}{c}\Delta, p \vdash p' \\ \Delta, q' \vdash p \twoheadrightarrow q\end{array}}{\Delta \vdash p \twoheadrightarrow q}\ (\twoheadrightarrow\text{I2}) \qquad \frac{\Delta \vdash p \twoheadrightarrow q \quad \Delta, q \vdash p}{\Delta \vdash q}\ (\twoheadrightarrow\text{E})$$

Figure 3: Natural deduction for PCL (rules for $\twoheadrightarrow$; the full set of rules is in [5]).

2.2 Propositional Contract Logic

We briefly review Propositional Contract Logic (PCL [11]), PCL extends intuitionistic propositional logic IPC with the connective $\twoheadrightarrow$, called *contractual implication*. We assume that the atoms of PCL are the events in E. The formulae of PCL are defined as follows:

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

A proof system for PCL is defined in [11] in terms of Gentzen-style rules (Fig. 2), which extend those of IPC. In all the rules, Δ is a set of PCL formulae. Decidability of PCL has been established in [11] by proving that the Gentzen-style proof system of PCL enjoys cut elimination and the subformula property.

In this paper we shall mainly consider the Horn fragment of PCL, which comprises atoms, conjunctions, and non-nested $\to$/$\twoheadrightarrow$ implications. Let α,β range over conjunctions of atoms. A *Horn* PCL *theory* is a set of clauses of the form $\alpha \to a$ or $\alpha \twoheadrightarrow a$. The clause a is a shorthand for $\top \to a$. We shall denote with $\overline{\alpha}$ the set of atoms in α.

3 Proof traces in PCL

In this section we introduce the notion of *proof traces*, namely the sequences of atoms respecting the order imposed by proofs in PCL. To do that, we first define a natural deduction system for PCL, which extends that of IPC with the rules in Fig. 3. 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 crucial rule is ($\twoheadrightarrow$E), which allows for the elimination of $\twoheadrightarrow$. Compared to the rule 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:*

$$\frac{\Delta \vdash b \twoheadrightarrow a \quad \dfrac{\Delta \vdash a \to b \quad \Delta, a \vdash a}{\Delta, a \vdash b}(\to\text{E})}{\Delta \vdash a}(\twoheadrightarrow\text{E})$$

The natural deduction system of Fig. 3 is equivalent to the Gentzen calculus of [11].

Theorem 3.2. *Thre exists a proof π of $\Delta \vdash p$ in natural deduction iff there exists a proof π^* of $\Delta \vdash p$ in the sequent calculus of [11].*

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

Figure 4: Proof traces of Horn PCL.

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

Lemma 3.3. *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), (∧I), (∧E1),(∧E2), (→E), *and* (↠E).

A key observation is that each proof in Horn PCL induces a set of atom orderings which are compatible with the proof. Each of these orderings is associated with a sequence of atoms, called *proof trace*. To give some intuition, consider the elimination rule for →:

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

The rule requires a proof of all the atoms in α in order to construct a proof of a. Accordingly, if σ is a proof trace of Δ, then σa if a proof trace of Δ.

Consider now the elimination rule for ↠

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

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, the proof traces of Δ include all the interleavings between σ and a.

Definition 3.4 (Proof traces)**.** *For a Horn* PCL *theory Δ, we define the set of sequences of atoms $[\![\Delta]\!]$ by the rules in Fig. 4. 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 operators remove duplicates from the right, e.g. $aba \mid ca = ab \mid ca = \{abc, acb, cab\}$. We call each $\sigma \in [\![\Delta]\!]$ a* proof trace *of Δ.*

Example 3.5. *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 Fig. 1). By Def. 3.4, 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:

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

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.

We now define, starting from a set X of atoms, which atoms may be proved immediately after while following some proof trace. We call these atoms *urgent*, and we denote with $\mathcal{U}_\Delta^X$ the set of urgent atoms in X. For instance, with Δ_1 in Ex. 3.5, we have $\mathcal{U}_{\Delta_1}^{\emptyset} = \{a\}$, $\mathcal{U}_{\Delta_1}^{\{a\}} = \{b\}$, $\mathcal{U}_{\Delta_1}^{\{b\}} = \{a\}$, and $\mathcal{U}_{\Delta_1}^{\{a,b\}} = \emptyset$.

Definition 3.6. *For a set $X \subseteq E$ and a Horn* PCL *theory Δ, we define $\mathcal{U}_\Delta^X$ as:*

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

Theorem 3.11 below characterizes urgent atoms in terms of provability. This is obtained by a suitable rewriting of Horn PCL theories, which separates the urgent atoms from the provable ones.

Technically, in Def. 3.7 we introduce 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 $\{\star e \mid e \in X\}$. We denote with $\mathit{atoms}(\Delta)$ the set of all atoms in Δ. We assume that $\mathit{atoms}(\Delta) \cap \star E = \emptyset$, 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 $\star\alpha = \star a_1 \wedge \cdots \wedge \star a_n$. When $n = 0$, $\star\alpha = \top$.

Definition 3.7. *The endomorphism $[\cdot]_\mathcal{U}$ of Horn* PCL *theories is defined as:*

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

Intuitively, the atoms of the form $!a$ correspond to actions already happened in the past, the atoms Ua correspond to the urgent actions (also including the past ones), while the atoms Ra are those actions which can be eventually reached by performing the urgent ones. 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 3.8. *For the* PCL *theory $\Delta_3 = \{a \to b,\ b \twoheadrightarrow a\}$ in Ex. 3.5, we have:*

$$\begin{aligned}
[\Delta_3]_\mathcal{U} \;=\; \{&!a \to Ub,\ \ Ra \to Rb,\ \ Rb \twoheadrightarrow Ua, \\
&!a \to Ua,\ \ !b \to Ub,\ \ Ua \to Ra,\ \ Ub \to Rb\}
\end{aligned}$$

We have that $[\Delta_3]_\mathcal{U} \vdash Ua$ and $[\Delta_3]_\mathcal{U} \nvdash Ub$; also, $[\Delta_3]_\mathcal{U}, !a \vdash Ub$. Notice that if the clause $b \twoheadrightarrow a$ were mapped by $[]_\mathcal{U}$ to $Rb \to Ua$ (without contractual implication), then no atoms would have been provable in $[\Delta_3]_\mathcal{U}$.

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

The following lemma relates proof traces with urgent atoms derivable from $[\Delta]_\mathcal{U}$. The ($\Leftarrow$) direction states that (any prefix of) a proof trace is made by urgent atoms in sequence. The ($\Rightarrow$) direction states that a sequence of urgent atoms can be extended to a proof trace.

Lemma 3.10. *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 $[\,]_{\mathcal{U}}$ follows. Given a Horn PCL theory Δ, an atom a is urgent in Δ iff Ua is provable in $[\Delta]_{\mathcal{U}}$.

Theorem 3.11. *For all Horn* PCL *theories* Δ*, and for all* $a \notin X \subseteq E$*:*

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

Proof. ($\Rightarrow$) Assume that $a \in \mathcal{U}_\Delta^X$. By Def. 3.6, there exist σ, σ' such that $\overline{\sigma} = X$ and $\sigma a \sigma' \in [\![\Delta, X]\!]$. By Lemma 3.10, we have $[\Delta, X]_{\mathcal{U}}, !X \vdash Ua$. The thesis $[\Delta]_{\mathcal{U}}, !X \vdash Ua$ follows because $[X]_{\mathcal{U}} = !\top \to UX$ and $!X$ implies UX.

($\Leftarrow$) Assume that $[\Delta]_{\mathcal{U}}, !X \vdash Ua$. Since $[\Delta, X]_{\mathcal{U}} \vdash Ue$ for all $e \in X$. Take any σ such that $\overline{\sigma} = X$. By Lemma 3.10 it follows that there exist σ, η such that $\overline{\sigma} = X$ and $\sigma a \eta \in [\![\Delta, X]\!]$. By Def. 3.6, we conclude that $a \in \mathcal{U}_\Delta^X$. □

4 A logical view of contracts

In this section we present our main results about the relation between contracts and PCL. For a conflict-free CES $\mathcal{E}$ and a Horn PCL theory Δ, we write $\Delta \sim \mathcal{E}$ whenever there exists an isomorphism 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 $(\bigwedge X) \twoheadrightarrow e$. Theorem 4.5 shows that, for a relevant class of payoff functions, we can characterise agreement in terms of provability in PCL. Theorem 4.9 states that proof traces correspond to sequences of prudent events. Finally, Theorem 4.11 relates winning strategies with urgent atoms.

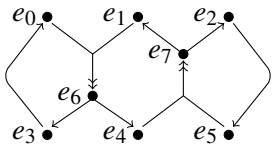
Before providing the technical details, we illustrate the relevance of these results with the help of a couple of examples.

Example 4.1. *Consider the following Horn* PCL *theory* $\Delta_\star$*:*

$$\begin{aligned}\Delta_\star = \{&(e_0 \wedge e_1) \twoheadrightarrow e_6,\ e_6 \to e_3,\ e_6 \to e_4,\ e_3 \to e_0,\\ &(e_4 \wedge e_5) \twoheadrightarrow e_7,\ e_7 \to e_1,\ e_7 \to e_2,\ e_2 \to e_5\}\end{aligned}$$

It is possible to prove that $\Delta_\star \vdash e_i$ *for all* $i \in 0..7$*. However, this is not straightforward to see, and indeed were any one of the* $\twoheadrightarrow$ *in* $\Delta_\star$ *replaced with a* $\to$*, then no atoms would have been provable.*

We can exploit the correspondence between provability in PCL *and agreement in contracts to obtain a simple proof of* $\Delta_\star \vdash e_i$*. To do that, observe that* $\Delta_\star$ *is isomorphic to the* CES $\mathcal{E}_\star$ *depicted as:*



and let $\mathcal{C} = \langle \mathcal{E}_\star, \Phi \rangle$*, where we assume a single participant* A*, whose payoff is* $\Phi \mathsf{A} = \{\sigma \mid \forall i \in 0..7.\ e_i \in \overline{\sigma}\}$.

It is easy to check that the contract $\mathcal{C}$ *admits an agreement. Indeed,* e_6 *and* e_7 *are prudent in* ε*;* e_0 *becomes prudent after* e_3 *is fired;* e_5 *after* e_2*; events* e_3, e_4 *after* e_6*; events* e_1, e_2 *after* e_7*. Therefore, there exists a winning strategy for* A *in* $\mathcal{C}$*. Theorem 4.5 allows for transferring this result back to* PCL*, by establishing that all the atoms* $e_0, \ldots, e_7$ *are provable in* $\Delta_\star$

Furthermore, the correspondence between contracts and PCL *allows for easily constructing the proof traces of $\Delta_\star$ — which is not as straightforward by applying Def. 3.4. The plays σ where* A *wins are those where only the prudent events are performed, i.e.:*

$$\sigma \in \big(e_6\,(e_4 \mid e_3 e_0)\big) \mid \big(e_7\,(e_1 \mid e_2 e_5)\big)$$

By Theorem 4.9, these plays exactly correspond to the proof traces of the PCL *theory $\Delta_\star$.*

Example 4.2 (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 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 $\{\vdash, \Vdash\}$. For all $\bullet \in \mathfrak{F}$, let $\mathcal{E}^\bullet$ be the CES*:*

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

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 $\bullet(i,j) = \Vdash$).

Now, let $\Phi(\mathsf{A}_{i,j}) = \{\sigma \mid \overline{\sigma} \cap E_{i,j} \geq 2\}$, 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 have 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 4.5 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.

Definition 4.3. *We write $\Delta \sim \mathcal{E}$ when $\mathcal{E}$ is conflict-free, and*

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

To relate agreement with provability, we consider the class of *reachability payoffs*, which neglect the order in which events are performed. This class is quite broad. For instance, it includes the *offer-request payoffs* [9]. Intuitively, these are used by participants which want to be paid for each provided service. Each participant A has a set $\{O^0_\mathsf{A}, O^1_\mathsf{A}, \ldots\}$ of sets of events (the *offers*), and a corresponding set $\{R^0_\mathsf{A}, R^1_\mathsf{A}, \ldots\}$ (the *requests*). To be winning, whenever A performs in a play some offer O^i_A (in whatever order), the play must also contain the corresponding request R^i_A, and at least one of the requests has to be fulfilled.

Definition 4.4. *A* reachability payoff *is a function* $\Phi : \mathcal{A} \to \wp(E^\infty)$ *such that if* $\overline{\sigma} = \overline{\eta}$ *then* $\sigma \in \Phi\mathsf{A} \iff \eta \in \Phi\mathsf{A}$*, for all* $\mathsf{A} \in \mathcal{A}$.

Alternatively, Φ is a reachability payoff when there exists some predicate $\varphi \subseteq \wp(E)$ such that $\sigma \in \Phi\mathsf{A}$ iff $\overline{\sigma} \in \varphi$, for all $\mathsf{A} \in \mathcal{A}$.

The following theorem gives a logical characterisation of agreements. If Φ is a reachability payoff induced by φ, and $\Delta \sim \mathcal{E}$, then the contract $\langle \mathcal{E}, \Phi \rangle$ admits an agreement whenever the set provable atoms in Δ satisfies the predicate φ.

Theorem 4.5. *Let* $\Delta \sim \mathcal{E}$*, and let* Φ *be a reachability payoff defined by the predicate* φ*. Then, the contract* $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ *admits an agreement iff* $\{a \mid \Delta \vdash a\} \in \varphi$.

Example 4.6. *Consider the following offer-request payoff* Φ *of* A *and* B*:*

$$O^0_\mathsf{A} = \{a_0\} \qquad O^1_\mathsf{A} = \{a_0, a_1\} \qquad O^0_\mathsf{B} = \{b_0\} \qquad O^1_\mathsf{B} = \{b_2\}$$
$$R^0_\mathsf{A} = \{b_0, b_2\} \qquad R^1_\mathsf{A} = \{b_1\} \qquad R^0_\mathsf{B} = \{a_0\} \qquad R^1_\mathsf{B} = \{a_0, a_2\}$$

and let the obligations of A *and* B *be modelled by the* CES $\mathcal{E}$ *with enablings:*

$$\{b_0, b_2\} \Vdash a_0 \quad b_1 \vdash a_1 \quad b_2 \Vdash a_2 \quad a_0 \vdash b_0 \quad \{a_0, a_1\} \vdash b_1 \quad \{a_0, a_2\} \vdash b_2$$

In the PCL *theory* $\Delta \sim \mathcal{E}$*, the set of provable atoms is* $\{a_0, a_2, b_0, b_2\}$*. Therefore, by Theorem 4.5 it follows that the contract* $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ *admits an agreement.*

Recall from Def. 2.8 that, when a contract admits an agreement, all participants have a winning strategy. Two relevant question are then how to construct a winning strategy for each participant, and how such strategy is related to PCL. We answer these questions in Theorem 4.11 below, where we show that a winning strategy can be obtained by following the order of urgent atoms.

In order to prove Theorem 4.11 we need to establish some further results about strategies and proof traces. The first result is Lemma 4.7, which provides an alternative characterisation of prudent events in case of conflict-free contracts. We denote with $\mathcal{R}^X$ the set *reachable events with past* X. Intuitively, if a set X of events has been performed in the past, we consider an event $e \notin X$ reachable with past X when e occurs in some play $\sigma\eta$ where the prefix σ is a linearization of X, and the overall credits are contained in X (i.e., past debits need not be honoured). Lemma 4.7 states that an event e is prudent for A in σ whenever $e \in \mathcal{P}^{\overline{\sigma}}$, namely the set of events which are $\vdash$-enabled by $\overline{\sigma}$, or $\Vdash$-enabled by $\overline{\sigma} \cup \mathcal{R}^{\overline{\sigma}}$.

Lemma 4.7. *For a set* $X \subseteq E$*, let*

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

Then, e *is prudent in* σ *iff* $e \in \mathcal{P}^{\overline{\sigma}}$.

The criterion given by Lemma 4.7 is much simpler than the mutually coinductive definition of prudence in Def. 2.5. Indeed, a polynomial-time algorithm for computing $\mathcal{P}^X$ can be easily devised as follows. At step 0, we compute the reflexive transitive closure X_1 of the hypergraph of the CES $\mathcal{E}$ (neglecting the $\Vdash$-enablings), taking as start nodes all the events in $X \cup Y_0$, where $Y_0 = \{e \mid \exists Z : Z \Vdash e \in \mathcal{E}\}$ contains the events at the right of some $\Vdash$ in $\mathcal{E}$. The transitive closure can be computed in polynomial time in the number of events in $\mathcal{E}$. If $X_1 \Vdash Y_0$, then $X_1 = \mathcal{R}^X$. Otherwise, we repeat the above procedure with start nodes $X \cup Y_1$, where $Y_1 = \{e \in Y_0 \mid X_1 \Vdash e\}$, until reaching a fixed point. In the worst case,

we do n steps, hence we have a polynomial algorithm for computing $\mathcal{R}^X$. After this, $\mathcal{P}^X$ can be easily computed, as in Lemma 4.7.

The following lemma provides a link between contracts and PCL, by establishing that prudent events in a CES $\mathcal{E}$ correspond exactly to urgent atoms in a PCL theory $\Delta \sim \mathcal{E}$. The idea of the proof is to exploit the mapping $[]_{\mathcal{U}}$ in Def. 3.7 as a bridge between CES and PCL. To do that, we first map $\mathcal{E}$ to a PCL theory $[\mathcal{E}]_{\mathcal{U}}$, and we relate the prudent events in $\mathcal{E}$ to the provable atoms in $[\mathcal{E}]_{\mathcal{U}}$. Since $\Delta \sim \mathcal{E}$, we have that $[\mathcal{E}]_{\mathcal{U}} = [\Delta]_{\mathcal{U}}$, and so by Theorem 3.11 we can relate provability in $[\Delta]_{\mathcal{U}}$ with urgent atoms in Δ. Summing up, the prudent events in $\mathcal{E}$ are the urgent atoms in Δ.

Lemma 4.8. *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 4.9 states that the plays of prudent events correspond to prefixes of proof traces.

Theorem 4.9. *Say $\sigma = \langle e_0 e_1 \cdots \rangle$ is a* prudent play *of $\mathcal{E}$ when e_i is prudent for σ_i in $\mathcal{E}$, for all i. If $\Delta \sim \mathcal{E}$, then σ is a prudent play of $\mathcal{E}$ iff $\exists \eta.\ \sigma\eta \in [\![\Delta]\!]$.*

Example 4.10. *The prudent plays of the* CES $\mathcal{E}_3$ *in Fig. 1 are ε, a, and ab (see Ex. 2.6). By Theorem 4.9, 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 Ex. 3.5).*

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.

5 Conclusions

We have studied the relations between two foundational models for contracts. The main result is that the notions of agreement and winning strategy in the game-theoretic model of [9] have been related, respectively, to that of provability and proof traces in the logical model of [11] (Theorems 4.5 and 4.11).

Some preliminary work on relating event structures with the logic PCL has been reported in [8]. The model of [8] does not exploit game-theoretic notions: 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 simplified 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 participant payoffs are provable. Theorem 4.5 extends this result to a more general (game-theoretic) notion of agreement and of payoff.

In [6] the idea of performing events "on credit" has been explored in the domain of Petri nets. In the variant of Petri nets presented in [6] (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. 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.

An encoding of Horn PCL formulae into a variant of CCS has been presented in [10]. 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 preserve the notion of culpability defined in the logical model. In particular, in the CCS model a participant has to be culpable only when omitting to produce a promised output, or omitting to input an available message.

References

[1] Wil M. P. van der Aalst, Niels Lohmann, Peter Massuthe, Christian Stahl & Karsten Wolf (2010): *Multiparty Contracts: Agreeing and Implementing Interorganizational Processes*. Comput. J. 53(1), pp. 90–106.

[2] Martín Abadi, Michael Burrows, Butler Lampson & Gordon Plotkin (1993): *A calculus for access control in distributed systems*. ACM TOPLAS 4(15).

[3] Martín Abadi & Gordon D. Plotkin (1993): *A Logical View of Composition*. Theoretical Computer Science 114(1).

[4] Michael Armbrust et al. (2010): *A view of cloud computing*. Comm. ACM 53(4), pp. 50–58.

[5] Massimo Bartoletti, Tiziana Cimoli, Paolo Di Giamberardino & Roberto Zunino: *Contract agreements via logic*. Available online at `tcs.unica.it/papers/ces-pcl-long.pdf`.

[6] Massimo Bartoletti, Tiziana Cimoli & G. Michele Pinna (2013): *Lending Petri nets and contracts*. In: Proc. FSEN. To appear.

[7] Massimo Bartoletti, Tiziana Cimoli, G. Michele Pinna & Roberto Zunino: *Circular causality in event structures*. Submitted. Available online at `tcs.unica.it/papers/ces-long.pdf`. A preliminary version of this paper has been presented at ICTCS 2012.

[8] Massimo Bartoletti, Tiziana Cimoli, G. Michele Pinna & Roberto Zunino (2012): *An event-based model for contracts*. In: Proc. PLACES.

[9] Massimo Bartoletti, Tiziana Cimoli & Roberto Zunino (2013): *A theory of agreements and protection*. In: Proc. POST, LNCS 7796, Springer.

[10] Massimo Bartoletti, Emilio Tuosto & Roberto Zunino (2012): *Contract-oriented Computing in CO_2*. Scientific Annals in Computer Science 22(1), pp. 5–60.

[11] Massimo Bartoletti & Roberto Zunino (2010): *A Calculus of Contracting Processes*. In: LICS, doi:10.1109/LICS.2010.25.

[12] Laura Bocchi, Kohei Honda, Emilio Tuosto & Nobuko Yoshida (2010): *A theory of design-by-contract for distributed multiparty interactions*. In: CONCUR, doi:10.1007/978-3-642-15375-4_12.

[13] Mario Bravetti, Ivan Lanese & Gianluigi Zavattaro (2008): *Contract-Driven Implementation of Choreographies*. In: Proc. TGC, pp. 1–18, doi:10.1007/978-3-642-00945-7_1.

[14] Mario Bravetti & Gianluigi Zavattaro (2007): *Contract Based Multi-party Service Composition*. In: Proc. FSEN, pp. 207–222, doi:10.1007/978-3-540-75698-9_14.

[15] Giuseppe Castagna, Nils Gesbert & Luca Padovani (2009): *A theory of contracts for Web services*. ACM TOPLAS 31(5), doi:10.1145/1538917.1538920.

[16] G. Decker, O. Kopp, F. Leymann & M Weske (2007): *BPEL4Chor: Extending BPEL for Modeling Choreographies*. In: Proc. ICWS.

[17] Jonathan Gelati, Antonino Rotolo, Giovanni Sartor & Guido Governatori (2004): *Normative autonomy and normative co-ordination: Declarative power, representation, and mandate*. Artificial Intelligence and Law 12(1-2).

[18] Thomas T. Hildebrandt & Raghava Rao Mukkamala (2010): *Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs*. In: *Proc. PLACES*.

[19] Kohei Honda, Aybek Mukhamedov, Gary Brown, Tzu-Chun Chen & Nobuko Yoshida (2011): *Scribbling Interactions with a Formal Foundation*. In: *Distributed Computing and Internet Technology*, *LNCS* 6536, Springer.

[20] Kohei Honda, Nobuko Yoshida & Marco Carbone (2008): *Multiparty asynchronous session types*. In: *POPL*.

[21] N. Kavantzas, D. Burdett, G. Ritzinger, T. Fletcher, Y. Lafon & C Barreto (2005): *Web Services Choreography Description Language V. 1.0*.

[22] Alessio Lomuscio, Wojciech Penczek, Monika Solanki & Maciej Szreter (2011): *Runtime Monitoring of Contract Regulated Web Services*. *Fundam. Inform.* 111(3).

[23] Cristian Prisacariu & Gerardo Schneider (2012): *A Dynamic Deontic Logic for Complex Contracts*. *The Journal of Logic and Algebraic Programming (JLAP)* 81(4).

[24] Franco Raimondi, James Skene & Wolfgang Emmerich (2008): *Efficient online monitoring of web-service SLAs*. In: *SIGSOFT FSE*.

[25] Richard Statman (1979): *Intuitionistic propositional logic is polynomial-space complete*. *Theoretical Computer Science* 9, pp. 67–72.

[26] Glynn Winskel (1986): *Event Structures*. In: *Advances in Petri Nets*, pp. 325–392.