Circular Causality in Event Structures

Massimo Bartoletti[∗]**, Tiziana Cimoli**[∗] **and G. Michele Pinna**[∗]

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

Roberto Zunino

Dipartimento di Matematica, Università degli Studi di Trento and COSBI, Italy

---

Abstract. We propose a model of events with circular causality, in the form of a conservative extension of Winskel's event structures. We study the relations between this new kind of event structures and Propositional Contract Logic. Provable atoms in the logic correspond to reachable events in our event structures. Furthermore, we show a correspondence between the configurations of this new brand of event structures and the proofs in a fragment of Propositional Contract Logic.

Keywords: Event structures, Contracts, Intuitionistic logic.

1. Introduction

Event structures (ES) are one of the classical model for concurrency, since [14, 21]. Notwithstanding the variety of ingredients appeared in the literature, ES are at least equipped with a relation (written $\vdash$ in [21]) modelling *causality*, and another one modeling non-determinism (usually rendered in terms of conflicts or consistency). Extensions to ES often use other relations to model other kind of dependencies, *e.g.* or-causality [3]. ES can provide a basic semantic model for concurrent systems, by interpreting the enabling $\{a\} \vdash b$ as: "event b can be done *after* after a has been done".

For instance, consider the following scenario. Alice has an apple, and Bob has a banana. The goal of Alice and Bob is to trade their goods. Since Alice and Bob do not trust each other, before exchanging their fruits they issue two *contracts*. The contract of Alice is formalised as an ES with enabling $\emptyset \vdash a$, meaning that Alice takes the first step in this trade, by giving the apple (modelled by event a) to Bob.

Bob's contract is an ES with enabling $\{a\} \vdash b$, meaning that Bob will wait for the apple, before giving Alice the banana (modelled by event b).

The composition of the above two contracts results in an ES $\mathcal{E}_0$ with enablings:

$$\mathcal{E}_0 : \qquad \emptyset \vdash a \qquad \{a\} \vdash b$$

Intuitively, in the composed contract Alice and Bob have an *agreement*, because when both participants behave as prescribed by their contracts, a configuration is reached where they both have fulfilled their objectives: Alice will receive a banana, and Bob will receive an apple. Technically, here the agreement is represented by the ES $\mathcal{E}_0$ having the configuration $\{a, b\}$.

However, it seems interesting to study which guarantees are provided by the two contracts considered in isolation; that is, we wonder what happens if a participant advertises her contract in an environment where (possibly malicious) participants can play arbitrary contracts. Intuitively, Bob is *protected* by his contract, because whatever opponent he interacts with, Bob will receive an apple before giving away his banana. Instead, Alice is *not* protected by her contract: indeed, the enabling $\emptyset \vdash a$ forces Alice to give her apple away even when nothing is expected in exchange.

Consider now a variant of the above scenario, where Alice changes her contract into $\{b\} \vdash a$. Now, the composition of Alice's and Bob's contracts is:

$$\mathcal{E}_1 : \qquad \{b\} \vdash a \qquad \{a\} \vdash b$$

Both participants are now protected, but an agreement is no longer possible: indeed, none of the events a or b will ever be enabled, because of the circularity between the requirements in the contracts. Technically, the only configuration of the ES $\mathcal{E}_1$ is the empty one.

A main result in [5] is that, in a model of contracts based on ES, agreement and protection are mutually exclusive: that is, whenever an agreement exists, some of the participants are not protected. Roughly, the problem is that, when the offers of the participants mutually depend on their requests, the participant which risks in doing the first step is not protected.

The solution proposed in [5] to reconcile agreements with protection is an extension of Winskel's ES, called *ES with circular causality* (in short, CES) with a new enabling relation, denoted by $\Vdash$. Intuitively, a circular enabling $\{b\} \Vdash a$ models that "event a can be done in exchange of the *promise* that b will eventually be done".

In our trading scenario, Alice can now revise her contract as $\{b\} \Vdash a$, which together with Bob's contract gives the CES:

$$\mathcal{E}_2 : \qquad \{b\} \Vdash a \qquad \{a\} \vdash b$$

Like in the scenario modelled by $\mathcal{E}_0$, Alice must take the first step. An agreement exists, because after Alice's first step, Bob is obliged to give her the banana (technically, $\{a, b\}$ will be a configuration of $\mathcal{E}_2$). However, differently from $\mathcal{E}_0$, Alice is now protected: when composed with a contract which does not promise b, Alices' contract $\{b\} \Vdash a$ will prescribe her no obligations.

Contribution.   In this paper we study event structures with circular causality from a foundational point of view. The structure of the paper follows.

Section 2 introduces CES, together with some illustrative examples.

In Section 3 we state some of their basic properties, and we relate them to Winskel's ES. In particular, we show that the configurations of CES still enjoy the coherence and finiteness properties of Winskel's ES, though they are not coincidence-free, which is correct from our point of view because of the presence of circular dependencies. For instance, the configurations of the CES $\mathcal{E}_2$ are the empty one and $\{a, b\}$; coincidence-freeness would have required an "intermediate" configuration which only contains one of the two events. The circular dependency between a and b requires that in a configuration where one of the two events happens, also the other one happens.

The behaviour of a CES $\mathcal{E}$ is characterised as a set of sets of events (denoted by $\mathcal{F}_{\mathcal{E}}$), which satisfies coherence and finiteness. Any set of sets enjoying such properties is called *quasi-family* of configurations. We show that for all quasi-families of configurations F, a CES $\hat{\mathcal{E}}(F)$ without $\vdash$-enablings exists the configurations of which are exactly those in F, that is $F = \mathcal{F}_{\hat{\mathcal{E}}(F)}$. This strengthens a result in [21], where an ES $\hat{\mathcal{E}}(F)$ is constructed from a family of configurations F (i.e. a quasi-family also satisfying coincidence-freeness) such that $\mathcal{F} = \mathcal{F}_{\hat{\mathcal{E}}(F)}$.

Section 4 studies reachable events, i.e. those events which belong to some configuration. In the case of conflict-free CES, we show an inductive characterisation of the reachable events, which coincides with the extensional one. We then present a polynomial-time algorithm for constructing the set of reachable events of finite, conflict-free CES.

Section 5 discusses operational semantics for CES. We first present an LTS where labels are events, and states are pairs (C, X) where C is the set of events fired so far, while X is the (least) set of events taken "on credit". For instance, in the CES $\mathcal{E}_2$ we can fire one of the two events a or b even in the absence of a causal justification, by recording it in the credits. This LTS allows for firing each event not in conflict with those already performed. Thus, we can obtain traces where the credits are not eventually honoured. For instance, in $\mathcal{E}_2$ the trace ab honours the credits, while ba does not. Intuitively, in the last trace b is not justified in the initial state, so we must take it on credit; the only way to remove it from the credits would be through a circular enabling of the form $X \Vdash b$, which is not present in $\mathcal{E}_2$. We then present a less liberal LTS as a refinement of the previous one where all and only those events which lead to honoured traces can be fired. The refined LTS preserves the reachable events.

In Section 6 we study some relations between CES and the Propositional Contract Logic (PCL) introduced in [7]. In particular, we present two encodings from CES to PCL. The first encoding $[\cdot]_{\mathcal{R}}$ maps conflict-free CES into Horn PCL theories. We show that an event is reachable in a CES $\mathcal{E}$ if and only if it is provable in PCL under the theory $[\mathcal{E}]_{\mathcal{R}}$. Together with the results from Section 4, this relation provides us with an polynomial-time algorithm for provability in Horn PCL theories (whereas provability in the general case is PSPACE-hard). The second encoding $[\cdot]_{\mathcal{F}}$, which also deals with conflicts, reduces the problem of deciding if a set of events is a configuration to provability in PCL, i.e. $C \in \mathcal{F}_{\mathcal{E}}$ if and only if C is provable in PCL under the theory $[\mathcal{E}, C]_{\mathcal{F}}$, and $[\mathcal{E}, C]_{\mathcal{F}}$ is consistent.

Finally, in Section 7 we conclude and discuss some related work.

Although our main motivation for introducing CES is to provide a semantical model of contracts, the present paper does not feature a theory of contracts. For instance, we do not formalise here the notion of contract composition, and those of agreement and protection intuitively presented above. Rather, in this paper we focus on CES as a concurrency model *by itself*, in the same spirit of other extensions of event structures, e.g. [8, 3]. The foundational results provided by this paper are exploited in [5, 9] to develop a theory of contracts based on CES, and in particular to formalise the notions of agreement and protection.

All the proofs of our statements are contained either in the main body of the paper, or in Appendixes.

2. Event structures with circular causality

Definition 2.1. An event structure with circular causality (CES) is a quadruple $\mathcal{E} = (E, \#, \vdash, \Vdash)$ where:

- E is a set of events,

- $\# \subseteq E \times E$ is an irreflexive and symmetric relation, called *conflict* relation. We say that a set $X \subseteq E$ is *conflict-free* ($CF(X)$ in symbols) whenever $\forall e, e' \in X. \neg(e\#e')$. We denote with *Con* the set $\{X \subseteq_{fin} E \mid CF(X)\}$,

- $\vdash \subseteq Con \times E$ is the *enabling* relation,

- $\Vdash \subseteq Con \times E$ is the *circular enabling* relation,

The relations $\vdash$ and $\Vdash$ are *saturated*, i.e. for all $X, Y \in Con$ and for $\circ \in \{\vdash, \Vdash\}$:

$$X \circ e \;\wedge\; X \subseteq Y \implies Y \circ e$$

We say that $\mathcal{E}$ is *finite* when E is finite; we say that $\mathcal{E}$ is *conflict-free* when the conflict relation is empty.

Notation 2.2. For a sequence $\sigma = \langle e_0\, e_1 \ldots \rangle$ (possibly infinite), we write $\overline{\sigma}$ for the set of events in σ. We write σ_i for the subsequence $\langle e_0 \ldots e_{i-1} \rangle$. If $\sigma = \langle e_0 \ldots e_n \rangle$ is finite, we write σe for the sequence $\langle e_0 \ldots e_n\, e \rangle$. The empty sequence is denoted by ε.

Notation 2.3. We adopt the following conventions: $\vdash e$ stands for $\emptyset \vdash e$; we write $a \vdash b$ for $\{a\} \vdash b$. For a finite, conflict-free set X, we write $X \vdash Y$ for $\forall e \in Y. X \vdash e$. For an infinite, conflict-free X, we write $X \vdash Y$ as a shorthand for $\exists X_0 \subseteq_{fin} X. X_0 \vdash Y$. All the abbreviations above also apply to $\Vdash$.

A configuration C is a "snapshot" of the behaviour of the system. In [22], a set of events C is a configuration if and only if for each event $e \in C$ it is possible to find a *trace for e in C*, *i.e.* a finite sequence of events containing e, which is closed under the enabling relation:

$$\forall e \in C. \; \exists \sigma = \langle e_0 \ldots e_n \rangle. \; e \in \overline{\sigma} \subseteq C \;\wedge\; \forall i \leq n. \; \{e_0, \ldots, e_{i-1}\} \vdash e_i$$

We refine the notion in [22] to deal with circular causality. Intuitively, for all events e_i in the sequence $\langle e_0 \ldots e_n \rangle$, e_i can either be $\vdash$-enabled by its predecessors, or $\Vdash$-enabled by the *whole* sequence, i.e.:

$$\forall e \in C. \; \exists \sigma = \langle e_0 \ldots e_n \rangle. \; e \in \overline{\sigma} \subseteq C \;\wedge\; \forall i \leq n. \; \big(\{e_0, \ldots, e_{i-1}\} \vdash e_i \;\vee\; \overline{\sigma} \Vdash e_i\big)$$

Clearly, the configurations of a CES without $\Vdash$-enablings are also configurations in the sense of [22], hence CES are a conservative extension of Winskel's general ES. Differently from ES, if C is a finite configuration of a CES, and σe is a trace for all the events in C, not necessarily σ is a trace for $C \setminus \{e\}$ (see *e.g.*, $\mathcal{E}_2$ in Fig. 1).

To allow for reasoning about sets of events which are not configurations, we introduce the auxiliary notion of *X-configuration* in Def. 2.4 below. In an *X-configuration* C, the set C can contain an event e even in the absence of a justification through a standard/circular enabling — provided that e belongs to the set X. This allows, given an X-configuration, to add/remove any event and obtain a Y-configuration, possibly with $Y \neq X$. We shall say that the events in X have been taken "on credit", to remark the fact that they may have been performed in the absence of a causal justification. Configurations (i.e. $\emptyset$-configurations) represent sets of events where all the credits have been "honoured".
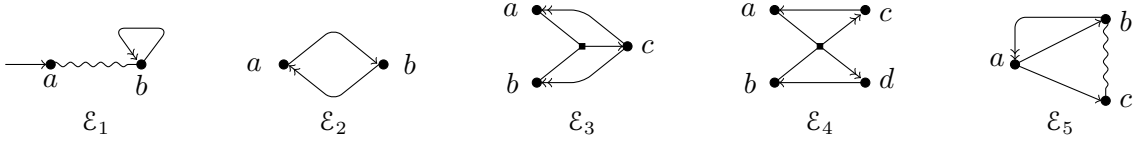
Figure 1. Five CES. We adopt the following graphical notation for depicting CES: they are denoted as directed hypergraphs, where nodes stand for events. An hyperedge from a set of nodes X to node e denotes an enabling $X \circ e$, where $\circ = \vdash$ if the edge has a single arrow, and $\circ = \Vdash$ if the edge has a double arrow. A conflict $a\#b$ is represented by a waved line between a and b.

Definition 2.4. (Traces and configurations)
Let $\mathcal{E} = (E, \#, \vdash, \Vdash)$ be a CES, and let $X \subseteq E$. A conflict-free sequence $\sigma = \langle e_0 \ldots e_n \rangle \in E^*$ without repetitions is an X-*trace* of $\mathcal{E}$ iff:

$$\forall i \leq n. \ (e_i \in X \ \lor \ \overline{\sigma_i} \vdash e_i \ \lor \ \overline{\sigma} \Vdash e_i) \tag{1}$$

For all $C, X \subseteq E$ we say that C is an X-*configuration of* $\mathcal{E}$ iff $CF(C)$ and:

$$\forall e \in C. \ \exists \sigma \ X\text{-trace}. \ e \in \overline{\sigma} \subseteq C \tag{2}$$

The set of all X-traces of $\mathcal{E}$ is denoted by $\mathcal{T}_\mathcal{E}(X)$, abbreviated as $\mathcal{T}_\mathcal{E}$ when $X = \emptyset$. The set of all X-configurations of $\mathcal{E}$ is denoted by $\mathcal{F}_\mathcal{E}(X)$, or just $\mathcal{F}_\mathcal{E}$ when $X = \emptyset$.

Example 2.5. Consider the five CES in Fig. 1.

(1) $\mathcal{E}_1$ has enablings $\vdash a$, $b \Vdash b$, and conflict $a\#b$. By Def. 2.4, $\emptyset, \{a\}, \{b\} \in \mathcal{F}_{\mathcal{E}_1}$, but $\{a, b\} \notin \mathcal{F}_{\mathcal{E}_1}$.

(2) $\mathcal{E}_2$ has enablings $a \vdash b$ and $b \Vdash a$. Here $\emptyset, \{a, b\} \in \mathcal{F}_{\mathcal{E}_2}$, while neither $\{a\}$ nor $\{b\}$ belong to $\mathcal{F}_{\mathcal{E}_2}$. Also, $\mathcal{F}_{\mathcal{E}_2}(\{b\}) = \{\emptyset, \{b\}, \{a, b\}\}$, and $\mathcal{F}_{\mathcal{E}_2}(\{a\}) = \{\emptyset, \{a\}, \{a, b\}\}$.

(3) $\mathcal{E}_3$ has enablings $\{a, b\} \vdash c$, $c \Vdash a$, and $c \Vdash b$. The only non-empty configuration of $\mathcal{E}_3$ is $\{a, b, c\}$.

(4) $\mathcal{E}_4$ has enablings $\{a, b\} \Vdash c$, $\{a, b\} \Vdash d$, $c \vdash a$, and $d \vdash b$. We have that $\{a, b, c, d\} \in \mathcal{F}_{\mathcal{E}_4}$. Note that, were one (or both) of the $\Vdash$ turned into a $\vdash$, then the only configuration would have been $\emptyset$.

(5) $\mathcal{E}_5$ has enablings $a \vdash b$, $a \vdash c$, $b \Vdash a$, and conflict $b\#c$. We have that $\{a, b\} \in \mathcal{F}_{\mathcal{E}_5}$ while $\{a, c\}$ is not a configuration, but it is an $\{a\}$-configuration.

Example 2.6. (Dining retailers [7])
Around a round table, n cutlery retailers are about to have dinner. At the center of the table, there is a large dish of food. Despite the food being delicious, the retailers cannot start eating right now. To do that, and follow the proper etiquette, each retailer needs a complete cutlery set, consisting of n pieces of different kinds. Each of the n retailers owns a distinct set of n pieces of cutlery, all of the same kind. The retailers start discussing about trading their cutlery, so that they can finally eat.

We formalise this scenario as follows. We name the retailers $A_1, \ldots, A_n$. Each retailer A_i initially owns n pieces of kind i. For all $j \neq i$, the event $e_{i,j}$ models A_i giving a piece of cutlery to retailer A_j.

Retailer A_i offers $n-1$ pieces of his cutlery (of kind i) in exchange for $n-1$ pieces of cutlery of the other kinds. The behaviour of retailer A_i is modelled by the following $n-1$ enablings:

$$A_i : \qquad \{e_{j,i} \mid j \neq i\} \Vdash e_{i,k} \qquad \text{for all } k \neq i$$

In the CES containing the enablings of all retailers, the set of events $E = \{e_{i,j} \mid i,j \in 1..n \text{ and } i \neq j\}$ is a configuration, hence each retailer can eventually eat. Note, instead, that any strict subset of E (except the empty one) is *not* a configuration. This models the fact that, once the retailers have started exchanging their cutlery, they are committed to continue until everyone can eat.

Following [22], we assume the *axiom of finite causes*, that is, we always require an event to be enabled by a *finite* chain of events. For instance, consider the event structure:

$$\cdots e_n \to \cdots e_3 \to e_2 \to e_1 \to e_0$$

For e_0 to happen, an infinite number of events must have happened *before* it. As in [22], we do not consider the set $\{e_i \mid i \geq 0\}$ as a configuration, because a justification of e_0 would require an infinite chain. Similarly, in the CES:

$$a_0 \leftarrow\mathrel{\mkern-14mu}\leftarrow a_1 \leftarrow\mathrel{\mkern-14mu}\leftarrow a_2 \leftarrow\mathrel{\mkern-14mu}\leftarrow a_3 \cdots \leftarrow\mathrel{\mkern-14mu}\leftarrow a_n \cdots$$

where, for a_0 to happen, an infinity of events must happen either *before* or *after* it, the set $\{a_i \mid i \geq 0\}$ is *not* a configuration according to Def. 2.4, because a justification of a_0 would require an infinite chain. This choice is motivated by the following (less abstract) example.

Example 2.7. (Money lender)
Suppose Bob has an old debt of €1 with Alice, but he has no money. Hence he asks Alice to lend him €1 to honour his debt. Alice agrees, provided that for this €1, Bob will give her back €2. When Bob receives the money, he honours his old debt, but now he owes Alice €2. Since he has no money, he asks again Alice to lend him €2. Alice agrees, provided that Bob will give her back €3. Every time he asks Alice to lend him €i, Alice requires him to give back €$(i+1)$. We can model this scenario as a CES with events a_i and b_i (for $i \geq 1$), where a_i represents Alice lending i euros to Bob, and b_i represents Bob giving i euros to Alice. The enablings are $b_{i+1} \Vdash a_i$ and $a_i \vdash b_i$, for all $i \geq 1$. Graphically:

$$b_1 \leftarrow a_1 \leftarrow\mathrel{\mkern-14mu}\leftarrow b_2 \leftarrow a_2 \leftarrow\mathrel{\mkern-14mu}\leftarrow b_3 \cdots$$

An *infinite* execution σ^∞ could have the form $\langle a_1\, b_1\, a_2\, b_2\, a_3\, b_3\, a_4\, b_4 \ldots\rangle$. Note that in σ^∞ each event a_i is $\Vdash$-enabled by $\sigma = \langle a_1 b_1 \ldots a_i b_i a_{i+1} b_{i+1}\rangle$, but σ is not a trace because a_{i+1} is not justified. Indeed, no finite subsequence σ of σ^∞ allows Bob to honour *all* the debts in σ. In the same spirit of [22], Def. 2.4 requires for each event in a configuration a *finite* justification, either in the past or in the future. Accordingly, $\overline{\sigma^\infty}$ is *not* a configuration.

3. Basic results on traces and configurations

In this section we study some basic properties of event structures with circular causality. Unless stated otherwise, in all the statements below in this section we assume a CES $\mathcal{E} = (E, \#, \vdash, \Vdash)$. When clear from the context, we will omit the index $\mathcal{E}$ from $\mathcal{F}_\mathcal{E}(X)$ and $\mathcal{T}_\mathcal{E}(X)$.

Definition 3.1. For all sequences σ, let $\sigma\downarrow$ be the sequence obtained by eliminating from σ all the duplicate events, starting from the right. Formally, we define $\sigma\downarrow$ inductively as follows:

$$\varepsilon\downarrow \;=\; \varepsilon \qquad\qquad (\sigma a)\downarrow \;=\; \sigma\downarrow \quad \text{if } a \in \overline{\sigma} \qquad\qquad (\sigma a)\downarrow \;=\; (\sigma\downarrow)\,a \quad \text{if } a \notin \overline{\sigma}$$

Every conflict-free sequence $\sigma\downarrow$ trivially belongs to $\mathfrak{T}(\overline{\sigma})$, which intuitively means that we can take every event on credit without worrying about $\vdash$ and $\Vdash$. The concatenation of two X-traces (modulo eliminating duplicated events) is an X-trace.

Lemma 3.2. For all $X, Y \subseteq E$, and for all $\sigma, \sigma' \in E^*$,

(a) $CF(\overline{\sigma}) \implies \sigma\downarrow \in \mathfrak{T}(\overline{\sigma})$

(b) $X \subseteq Y \implies \mathfrak{T}(X) \subseteq \mathfrak{T}(Y)$

(c) $\sigma \in \mathfrak{T}(X) \;\wedge\; \sigma' \in \mathfrak{T}(X) \;\wedge\; CF(\overline{\sigma\sigma'}) \implies (\sigma\sigma')\downarrow \in \mathfrak{T}(X)$

Proof:
Direct consequence of equation (1) in Def. 2.4. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ □

Since every event in a (possibly infinite) configuration is justified by a (finite) trace, for each finite subset C_0 of a configuration we can concatenate the traces of all the events in C_0, and still obtain a trace.

Lemma 3.3. For all $C, X \subseteq E$:

$$C \in \mathfrak{F}(X) \iff \forall C_0 \subseteq_{\mathit{fin}} C.\, \exists \sigma \in \mathfrak{T}(X).\, C_0 \subseteq \overline{\sigma} \subseteq C$$

Proof:
($\Rightarrow$) Let $C \in \mathfrak{F}(X)$, and let $C_0 \subseteq_{\mathit{fin}} C$. By Def. 2.4, $CF(C)$ and $\forall e \in C_0.\, \exists \sigma^e \in \mathfrak{T}(X).\, e \in \overline{\sigma^e} \subseteq C$. Since C_0 is finite, we can concatenate all the (finite, conflict-free) sequences σ^e obtained above. Let σ' be the result of such operation, and let $\sigma = \sigma'\downarrow$. By iterating 3.2(c) $|C_0|$ times, we obtain $\sigma \in \mathfrak{T}(X)$. Also, by construction we have that $C_0 \subseteq \overline{\sigma} \subseteq C$, from which the thesis follows.

($\Leftarrow$) Assume that $\forall C_0 \subseteq_{\mathit{fin}} C.\, \exists \sigma \in \mathfrak{T}(X).\, C_0 \subseteq \overline{\sigma} \subseteq C$, and let $e \in C$. By the hypothesis, since $\{e\} \subseteq_{\mathit{fin}} C$, there exists $\sigma^e \in \mathfrak{T}(X)$ such that $e \in \overline{\sigma^e} \subseteq C$. It remains to prove that $CF(C)$. By contradiction, assume that $\neg CF(C)$. Then, there would exist $C_0 \subseteq_{\mathit{fin}} C$ such that $\neg CF(C_0)$, and so by hypothesis there would also exist some $\sigma \in \mathfrak{T}(X)$ with $C_0 \subseteq \overline{\sigma}$. By (1), it must be $CF(\overline{\sigma})$, which contradicts $\neg CF(C_0)$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ □

From Lemma 3.3, we have that when an X-configuration C is finite, there exists an X-trace which covers all the events of C.

Corollary 3.4. For C a finite set of events, $C \in \mathfrak{F}(X)$ iff there exists $\sigma \in \mathfrak{T}(X)$ such that $\overline{\sigma} = C$.

If we interpret $\mathfrak{T}$ as a function from sets of events to sets of traces, we observe that $\mathfrak{T}$ is monotonic, i.e. for each $X \subseteq Y$ we have $\mathfrak{T}(X) \subseteq \mathfrak{T}(Y)$. Informally, this means that we can arbitrarily enlarge the credit set of a trace. On the contrary, we cannot reduce the credit set while preserving the traces; for instance in the CES $\vdash a,\, a \vdash b$, we have that $\langle ba \rangle$ is a $\{b\}$- trace but not a $\emptyset$-trace. For each trace σ there exists a *least* set X such that $\sigma \in \mathfrak{T}(X)$. This set is constructed as shown below.

Lemma 3.5. Let $\sigma = \langle e_0\, e_1\, \ldots\, e_n \rangle \in E^*$ be a conflict-free sequence without repetitions, and let $X = \{e_i \in \overline{\sigma} \mid \overline{\sigma_i} \nvdash e_i \wedge \overline{\sigma} \nVdash e_i\}$. Then X is the *least credit* for σ, i.e. $\sigma \in \mathcal{T}(X)$ and for all Y such that $\sigma \in \mathcal{T}(Y)$, we have $X \subseteq Y$.

Proof:
Let $\sigma = \langle e_0 \ldots e_n \rangle$, and let $X = \{e_i \in \overline{\sigma} \mid \overline{\sigma_i} \nvdash e_i \wedge \overline{\sigma} \nVdash e_i\}$. By Def. 2.4, it is easy to check that $\sigma \in \mathcal{T}(X)$. We will prove that $X \subseteq X'$ whenever $\sigma \in \mathcal{T}(X')$. Assume by contradiction that there exists $e \in X$ such that $e \notin X'$. By construction we have that $X \subseteq \overline{\sigma}$, thus there exists i such that $e_i = e$. Since $\sigma \in \mathcal{T}(X')$, by Def. 2.4 it follows that $\overline{\sigma_i} \vdash e_i$ or $\overline{\sigma} \Vdash e_i$, which contradicts the hypothesis. $\qquad\square$

The following lemma establishes a sufficient condition for preserving the credit set, when appending a trace to another.

Lemma 3.6. Let $\sigma \in \mathcal{T}(X)$ and $\eta \in \mathcal{T}(X \cup Y)$ be such that and $CF(\overline{\sigma}\,\overline{\eta})$. If $Y \subseteq \overline{\sigma}$, or $\overline{\sigma} \vdash Y$, or $\overline{\sigma} \Vdash Y$, then $(\sigma\,\eta)\!\downarrow\, \in \mathcal{T}(X)$.

Proof:
Let $\sigma = \langle e_0 \ldots e_n \rangle$, and let $\chi = (\sigma\,\eta)\!\downarrow = \sigma\,\langle e_{n+1} \ldots e_m \rangle$, where $\{e_{n+1}, \ldots, e_m\} = \overline{\eta} \setminus \overline{\sigma}$. By Def. 2.4 we have to prove that, for all $i \leq m$, $e_i \in X \vee \overline{\chi_i} \vdash e_i \vee \overline{\chi} \Vdash e_i$. We have the following two cases:

- $0 \leq i \leq n$. Here we can justify e_i in χ as it has been justified in σ.

- $n < i \leq m$. Here the only relevant case is when e_i has been justified by $e_i \in Y \setminus X$. Indeed, in all the other cases we can justify e_i in χ as it has been justified in η, by noting that $\overline{\chi_i} \supseteq \overline{\eta_{i-n}}$ and that the operator $\downarrow$ preserves the order of events. By hypothesis we have $Y \subseteq \overline{\sigma}$ or $\overline{\sigma} \vdash Y$ or $\overline{\sigma} \Vdash Y$. In the first case, by definition of $\downarrow$ it cannot be the case that $e_i \in Y$, for any $i > n$. In the second case, e_i can be justified by $\overline{\sigma} \vdash Y$. In the third case, e_i can be justified by $\overline{\sigma} \Vdash Y$.
$\qquad\square$

We now study properties of configurations. Some of them derive immediately from analogous properties of traces. Every set of conflict-free events X is an X-configuration; if $\mathcal{F}$ is interpreted as a function from sets of events to sets of sets of events, then $\mathcal{F}$ is monotonic, i.e. $\mathcal{F}(X) \subseteq \mathcal{F}(Y)$ whenever $X \subseteq Y$.

Lemma 3.7. For all $X, Y \subseteq E$:

(a) $CF(X) \implies X \in \mathcal{F}(X)$,

(a) $X \subseteq Y \implies \mathcal{F}(X) \subseteq \mathcal{F}(Y)$

Proof:
For (3.7), for all e in X, let $\sigma^e = \langle e \rangle$. It is immediate to check that $\sigma^e \in \mathcal{T}(X)$ and $e \in \overline{\sigma^e} \subseteq X$, and so $X \in \mathcal{F}(X)$. For (3.7), since $X \subseteq Y$, then each event e justified with $e \in X$ in equation (1) can also be justified with $e \in Y$, hence the thesis. $\qquad\square$

Differently from what happens in traces, in general for configurations there exists no *least* set X such that $C \in \mathcal{F}_\mathcal{E}(X)$, as a single configuration may have many *different* minimal credit sets. For instance, in a CES $\mathcal{E}$ with enablings $a \vdash b$, $b \vdash a$, we have that $\{a, b\} \in \mathcal{F}_\mathcal{E}(\{a\})$ and $\{a, b\} \in \mathcal{F}_\mathcal{E}(\{b\})$, but $\{a, b\} \notin \mathcal{F}_\mathcal{E}(\emptyset)$. The sets $\{a\}$ and $\{b\}$ are *minimal credits* for $\{a, b\}$, but there exists no least credit.

Lemma 3.8. If $C \in \mathcal{F}(X \cup Y)$ and $C \Vdash Y$, then $C \in \mathcal{F}(X)$.

Proof:
Let $e \in C$. Since $C \in \mathcal{F}(X \cup Y)$, there exists $\eta \in \mathcal{T}(X \cup Y)$ such that $e \in \overline{\eta} \subseteq C$. Since $C \Vdash Y$, by Notation 2.3 there exists a finite subset Z of C such that $Z \Vdash Y$. Since $Z \subseteq_{fin} C \in \mathcal{F}(X \cup Y)$, by Lemma 3.3 there exists $\sigma \in \mathcal{T}(X \cup Y)$ such that $Z \subseteq \overline{\sigma} \subseteq C$. Let $\chi = (\sigma\,\eta)\!\downarrow$. By Lemma 3.2(c), $\chi \in \mathcal{T}(X \cup Y)$. By saturation, since $Z \Vdash Y$ and $Z \subseteq \overline{\chi}$ we also have that $\overline{\chi} \Vdash Y$. By Lemma 3.5, it follows that $\chi \in \mathcal{T}(X)$. Since $e \in \overline{\chi} \subseteq C$, we have the thesis. $\qquad\square$

    The following lemma allows for simplifying the credit set when joining two configurations. In item (a), we have an X-configuration C and an $X \cup C$-configuration C'. We can then prove that $C \cup C'$ is an X-configuration: intuitively, the events in C' that were taken on credit from C can be justified with the credit set X alone, since $C \in \mathcal{F}(X)$. In item (b), we have an X-configuration C and an $X \cup Y$-configuration C' where $C \vdash Y$. We can then prove that $C \cup C'$ is an X-configuration: in a trace, to justify an event e taken on credit from Y, we can posticipate e after the finite subset of C which entails it. Since $C \in \mathcal{F}(X)$, this only requires to take on credit the set X. Item (c) is similar to the previous one, except that now we deal with a circular enabling. We have an $X \cup C'$-configuration C and an $X \cup Y$-configuration C' where $C \Vdash Y$. We can then prove that $C \cup C'$ is an X-configuration: all the events in Y will be justified by C, and since C is justified by C', $C \cup C'$ only requires to take on credit the set X.

Lemma 3.9. For all $C, C', X, Y \subseteq E$ such that $CF(C \cup C')$:

(a) $C \in \mathcal{F}(X) \ \wedge \ C' \in \mathcal{F}(X \cup C) \ \implies \ C \cup C' \in \mathcal{F}(X)$

(b) $C \in \mathcal{F}(X) \ \wedge \ C' \in \mathcal{F}(X \cup Y) \ \wedge \ C \vdash Y \implies C \cup C' \in \mathcal{F}(X)$

(c) $C \in \mathcal{F}(X \cup C') \ \wedge \ C' \in \mathcal{F}(X \cup Y) \ \wedge \ C \Vdash Y \implies C \cup C' \in \mathcal{F}(X)$

Proof:
For item (a), let $e \in C'$. Since $C' \in \mathcal{F}(X \cup C)$, Def. 2.4 prescribes that there exists $\sigma^e = \langle e_0 \dots e_n \rangle \in \mathcal{T}(X \cup C)$ such that $e \in \overline{\sigma^e} \subseteq C'$, i.e.:

$$CF(\overline{\sigma^e}) \ \wedge \ \forall i \leq n. \ (e_i \in X \cup C \ \vee \ \overline{\sigma_i^e} \vdash e_i \ \vee \ \overline{\sigma^e} \Vdash e_i)$$

Let Z_e be the set of e_i in σ^e for which the hypothesis $e_i \in C \setminus X$ has been used, i.e.:

$$Z_e \ = \ \{e_i \in \overline{\sigma^e} \mid e_i \in C \setminus X \ \wedge \ \overline{\sigma_i^e} \nvdash e_i \ \wedge \ \overline{\sigma^e} \nVdash e_i\}$$

Observe that $\sigma^e \in \mathcal{T}(X \cup Z_e)$. Since $Z_e \subseteq_{fin} C \in \mathcal{F}(X)$, by Lemma 3.3 there exists $\eta \in \mathcal{T}(X)$ such that $Z_e \subseteq \overline{\eta} \subseteq C$. Let $\chi = (\eta\,\sigma^e)\!\downarrow$. Since $\overline{\chi} \subseteq C \cup C'$ and $CF(C \cup C')$ by hypothesis, then $CF(\overline{\chi})$. Since $Z_e \subseteq \overline{\eta}$, Lemma 3.6 gives $\chi \in \mathcal{T}(X)$. Since $e \in \overline{\chi} \subseteq C \cup C'$, we have then proved (2), from which we conclude that $C \cup C' \in \mathcal{F}(X)$.

    For item (b), let $e \in C \cup C'$. We have two cases. If $e \in C$, then the hypothesis $C \in \mathcal{F}(X)$ directly gives a trace which satisfies equation (1). So, let $e \in C'$. Since $C' \in \mathcal{F}(X \cup Y)$, Def. 2.4 prescribes that there exists $\sigma^e \in \mathcal{T}(X \cup Y)$ such that $e \in \overline{\sigma^e} \subseteq C'$. Notice that $\sigma^e \in \mathcal{T}(X \cup (Y \cap \overline{\sigma^e}))$. Since $C \vdash Y$, then $C \vdash Y \cap \overline{\sigma^e}$. Then, by Notation 2.3 there exists a finite subset Z of C such that $Z \vdash Y \cap \overline{\sigma^e}$. Since

$Z \subseteq_{fin} C \in \mathcal{F}(X)$, by Lemma 3.3 there exists $\eta \in \mathcal{T}(X)$ such that $Z \subseteq \overline{\eta} \subseteq C$. By saturation, since $Z \vdash Y \cap \overline{\sigma^e}$ and $Z \subseteq \overline{\eta}$ we also have that $\overline{\eta} \vdash Y \cap \overline{\sigma^e}$. Therefore, Lemma 3.6 gives that $(\eta \, \sigma^e) \downarrow \in \mathcal{T}(X)$. Since $e \in \overline{(\eta \, \sigma^e) \downarrow} \subseteq C \cup C'$, we conclude that $C \cup C' \in \mathcal{F}(X)$.

For item (c), Lemma 3.7(3.7) yields $C \in \mathcal{F}(X \cup Y \cup C')$. Since $CF(C \cup C')$, by item (a) it follows that $C \cup C' \in \mathcal{F}(X \cup Y)$. Since $C \cup C' \Vdash Y$, by Lemma 3.8 we conclude that $C \cup C' \in \mathcal{F}(X)$. □

We relate Winskel's ES with CES in Th. 3.14 below. First, we introduce the needed definitions.

Definition 3.10. (Pairwise compatibility)
Let $\mathcal{F}$ be a family of sets. We say a subset $\mathcal{A}$ of $\mathcal{F}$ is *pairwise compatible* [1] if and only if

$$\forall e, e' \in \bigcup \mathcal{A}. \ \exists C \in \mathcal{F}. \ e, e' \in C$$

Definition 3.11. (Families and quasi-families of configurations)
For a set of sets $\mathcal{F}$ we define the following three properties:

Coherence If $\mathcal{A}$ is a pairwise compatible subset of $\mathcal{F}$, then $\bigcup \mathcal{A} \in \mathcal{F}$.

Finiteness $\forall C \in \mathcal{F}. \ \forall e \in C. \ \exists C_0 \in \mathcal{F}. \ e \in C_0 \subseteq_{fin} C$

Coincidence-freeness

$$\forall C \in \mathcal{F}. \ \forall e, e' \in C. \ \big(e \neq e' \implies (\exists C' \in \mathcal{F}. \ C' \subseteq C \ \wedge \ (e \in C' \iff e' \notin C')) \big)$$

We say that $\mathcal{F}$ is a *quasi-family of configurations* iff it satisfies coherence and finiteness; if $\mathcal{F}$ also satisfies coincidence-freeness, then we call $\mathcal{F}$ a *family of configurations*. In that case, we say that $\mathcal{F}$ is a family of configurations of E when $\bigcup \mathcal{F} = E$.

A basic result of [22] is that the set of configurations of an ES forms a family of configurations. On the contrary, the set of configurations of a CES does not satisfy *coincidence-freeness*. A counterexample is the CES $\mathcal{E}_2$ in Ex. 2.5(2), where $\{a, b\} \in \mathcal{F}$, but there exists no configuration including only a or b. Indeed, the absence of coincidence-freeness is a peculiar aspect of circularity: if two events are circularly dependent, each configuration that contains one of them must contain them both.

Theorem 3.12. For all CES $\mathcal{E}$, and for all $X \subseteq E$, the set $\mathcal{F}_{\mathcal{E}}(X)$ is a quasi-family of configurations.

Proof:
For coherence, let $\mathcal{A} \subseteq \mathcal{F}(X)$ be pairwise compatible in $\mathcal{F}(X)$. By Def. 3.10:

$$\forall e, e' \in \bigcup \mathcal{A}. \ \exists C \in \mathcal{F}(X). \ e, e' \in C$$

---

[1] Note that our definition differs from Winskel's (Def. 3.4 in [22]). There, a set $\mathcal{A} \subseteq \mathcal{F}$ is pairwise compatible iff for all $C, C' \in \mathcal{A}$, there exists $D \in \mathcal{F}$ such that $C \cup C' \subseteq D$. Clearly, Winskel's pairwise compatibility implies ours, while the converse is not true. For instance, consider the family of sets $\mathcal{A} = \{\emptyset, \{e_0\}, \{e_1\}, \{e_0, e_1\}, \{e_0, e_2\}, \{e_1, e_2\}\}$. Then, $\mathcal{A}$ is pairwise compatible according to Def. 3.10, while it is not according to Winskel's, because there exists no $D \in \mathcal{F}$ such that $\{e_0\} \subseteq D$ and $\{e_1, e_2\} \in D$. Clearly, both definitions imply that if $\mathcal{A}$ is pairwise compatible, then $\bigcup \mathcal{A}$ is conflict-free.

Since $C \in \mathcal{F}(X)$ implies $CF(C)$, it follows that $\neg(e\#e')$ for all $e, e' \in \bigcup\mathcal{A}$, and so $CF(\bigcup\mathcal{A})$. Let $e \in \bigcup\mathcal{A}$. Then, there exists $C \in \mathcal{A}$ such that $e \in C$. Since $C \in \mathcal{F}(X)$, by Def. 2.4 there exists $\sigma \in \mathcal{T}(X)$ such that $e \in \overline{\sigma} \subseteq_{fin} C$. Since $C \subseteq \bigcup\mathcal{A}$, by Def. 2.4 we can conclude that $\bigcup A \in \mathcal{F}(X)$.

Finiteness is straightforward by Def. 2.4, since for all $e \in C \in \mathcal{F}(X)$, the set of elements of the (finite) sequence $\sigma \in \mathcal{T}(X)$ such that $e \in \overline{\sigma} \subseteq_{fin} C$ is a configuration in $\mathcal{F}(X)$. $\qquad\square$

Despite faithfully representing the legitimate states of a system where all the credits are honoured, sets of configurations are not a precise semantic model for CES. Indeed, they are not able to discriminate among substantially different CES, e.g. like the following:

$$\mathcal{E}: \quad a \Vdash b, \ b \Vdash a \qquad \mathcal{E}': \quad a \vdash b, \ b \Vdash a \qquad \mathcal{E}'': \quad a \Vdash b, \ b \vdash a$$

It is easy to check that the sets of X-configurations of $\mathcal{E}, \mathcal{E}', \mathcal{E}''$ coincide, for all X. This contrasts with the different intuitive meaning of $\vdash$ and $\Vdash$, which is revealed instead by observing the traces:

$$\mathcal{T}_\mathcal{E} = \{\langle ab\rangle, \langle ba\rangle\} \qquad \mathcal{T}_{\mathcal{E}'} = \{\langle ab\rangle\} \qquad \mathcal{T}_{\mathcal{E}''} = \{\langle ba\rangle\}$$

To substantiate our feeling that configurations alone are not sufficiently discriminating for CES, in Theorem 3.14 we show that for all CES $\mathcal{E}$ there exists a CES $\mathcal{E}'$ *without $\vdash$-enablings* which has exactly the same configurations of $\mathcal{E}$. Therefore, the meaning of $\vdash$, that is the partial ordering of events, is completely lost by just observing configurations.

Definition 3.13. Let $\mathcal{F}$ be a quasi-family of configurations of a set E. We define the CES $\hat{\mathcal{E}}(\mathcal{F}) = (E, \#, \emptyset, \Vdash)$ as follows:

(a) $e\#e' \iff \forall C \in \mathcal{F}.\ e \notin C \lor e' \notin C$

(b) $X \Vdash e \iff CF(X) \land X$ is finite $\land \exists C \in \mathcal{F}.\ e \in C \subseteq X \cup \{e\}$

Theorem 3.14. For all quasi-families of configurations $\mathcal{F}$, we have $\mathcal{F}_{\hat{\mathcal{E}}(\mathcal{F})} = \mathcal{F}$.

Proof:
Let $\mathcal{F}$ be a quasi-family of configurations.

For $(\subseteq)$, let $C \in \mathcal{F}_{\hat{\mathcal{E}}(\mathcal{F})}$. By Def. 2.4 we have $CF(C)$, and for all $e \in C$ there exists C_e such that $e \in C_e \subseteq_{fin} C$, and the elements of C_e can be ordered as a trace in $\mathcal{T}_{\hat{\mathcal{E}}(\mathcal{F})}$. Since $\hat{\mathcal{E}}(\mathcal{F})$ has circular enablings only, it must be $\forall a \in C_e.\ C_e \Vdash a$. Hence, by Def. 3.13(b),

$$\forall a \in C_e.\ \exists D_a \in \mathcal{F}.\ a \in D_a \subseteq C_e \cup \{a\} = C_e$$

Since $\bigcup\{D_a \mid a \in C_e\} = C_e$, the set $\{D_a \mid a \in C_e\}$ is pairwise compatible in $\mathcal{F}$, hence by Theorem 3.12 (coherence) we have that $C_e = \bigcup\{D_a \mid a \in C_e\} \in \mathcal{F}$. Again, the set $\{C_e \mid e \in C\}$ is pairwise compatible in $\mathcal{F}$, therefore by coherence $C = \bigcup\{C_e \mid e \in C\} \in \mathcal{F}$.

For $(\supseteq)$, let $C \in \mathcal{F}$. By the definition of conflict in Def. 3.13(a), it must be $CF(C)$. By Theorem 3.12 (finiteness) for all $e \in C$ there exists $C_e \in \mathcal{F}$ such that $e \in C_e \subseteq_{fin} C$. For all $a \in C_e$, we have that $a \in C_e \subseteq C_e \cup \{a\} = C_e$. Thus, by Def. 3.13(b) it follows that $C_e \Vdash a$. Since this holds for all $a \in C_e$, by Def. 2.4 any ordering σ_e of the elements of C_e is a trace in $\mathcal{T}_{\hat{\mathcal{E}}(\mathcal{F})}$. Therefore, for all $e \in C$ we have found a trace $\sigma_e \in \mathcal{T}_{\hat{\mathcal{E}}(\mathcal{F})}$ such that $e \in \overline{\sigma_e} = C_e \subseteq C$. By Def. 2.4, we conclude that $C \in \mathcal{F}_{\hat{\mathcal{E}}(\mathcal{F})}$. $\qquad\square$

Corollary 3.15. For all ES $\mathcal{E}$, there exists a CES $\mathcal{E}'$ without $\vdash$-enablings such that $\mathcal{F}_\mathcal{E} = \mathcal{F}_{\mathcal{E}'}$.

4. Reachable events

Reachable events are those which belong to a configuration. More precisely, an event is X-reachable when some X-configuration contains it.

Definition 4.1. (Reachable events)
For all CES $\mathcal{E}$, we define the function $\mathcal{R}_{\mathcal{E}} : \wp(E) \to \wp(E)$ as:

$$\mathcal{R}_{\mathcal{E}}(X) = \bigcup \mathcal{F}_{\mathcal{E}}(X)$$

We say an event e X-*reachable* whenever $e \in \mathcal{R}_{\mathcal{E}}(X)$; we say e *reachable* when $e \in \mathcal{R}_{\mathcal{E}}(\emptyset)$. When clear from the context, we will omit the index $\mathcal{E}$ from $\mathcal{R}_{\mathcal{E}}(X)$, and just write $\mathcal{R}$ for $\mathcal{R}(\emptyset)$.

Example 4.2. Consider the CES $\mathcal{E}_2$ in Fig. 1, with enablings $a \vdash b$ and $b \Vdash a$. Since $\{a, b\}$ is a configuration, then $\mathcal{R}(\emptyset) = \{a, b\}$. Consequently, both a and b are X-reachable for all X.

Notice that there may not exist a least X such that $e \in \mathcal{R}(X)$. For instance, in the CES with enablings $a \vdash b$, $b \vdash a$, we have that a is both $\{a\}$-reachable and $\{b\}$-reachable, but it is not $\emptyset$-reachable.
The function $\mathcal{R}$ enjoys the following basic properties:

Lemma 4.3. For all $X, Y, C \subseteq E$:

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

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

(c) $C \subseteq \mathcal{R}(X) \wedge \mathit{CF}(\mathcal{R}(C \cup X)) \implies \mathcal{R}(X) = \mathcal{R}(C \cup X)$.

Item (a) is straightforward. Item (b) establishes the monotonicity of $\mathcal{R}$, which directly follows from the monotonicity of $\mathcal{F}$. From item (b), it follows that $\mathcal{R}(X) \cup \mathcal{R}(Y) \subseteq \mathcal{R}(X \cup Y)$, for all $X, Y \subseteq E$. Note that, in general, the converse does not hold: for instance consider the CES with enablings $\{e_1, e_2\} \Vdash a$, $e_1 \Vdash b$ and $e_2 \Vdash c$; then we have $\mathcal{R}(\{e_1\}) = \{e_1, b\}$, $\mathcal{R}(\{e_2\}) = \{e_2, c\}$ and $\mathcal{R}(\{e_1, e_2\}) = \{e_1, e_2, a, b, c\}$. Item (c) states that if C is X-reachable, then the set of X-reachable events equals to the set of $X \cup C$-reachable events. For instance, in the CES with enablings $a \vdash b$, $b \vdash c$, we have that $b \in \mathcal{R}(\{a\})$, hence $\mathcal{R}(\{a\}) = \mathcal{R}(\{a, b\})$. Note that when choosing $C = \mathcal{R}(X)$ in item (c), it follows that $\mathcal{R}(X)$ is a fixed point of $\mathcal{R}$, i.e. $\mathcal{R}(X) = \mathcal{R}(\mathcal{R}(X))$, provided that the set $\mathcal{R}(\mathcal{R}(X))$ is conflict-free.

Example 4.4. Consider the first three CES in Fig. 2.

(1) In $\mathcal{E}_6$, we have $\mathcal{R}(\emptyset) = \emptyset$, and $\mathcal{R}(\{a\}) = \{a, b\}$. Note that if one weakens the conflict-freeness requirement in Lemma 4.3(c), and only require $\mathit{CF}(C \cup X)$, then the thesis would no longer hold. Indeed, by choosing $C = \{a, b\}$ and $X = \{a\}$, we have $\mathcal{R}(X) = \{a, b\}$ and $\mathcal{R}(C \cup X) = \{a, b, c\}$, which is not conflict-free. Hence Lemma 4.3(c) does not apply, and in fact $\mathcal{R}(X) \neq \mathcal{R}(C \cup X)$.

(2) In $\mathcal{E}_7$, we have $\mathcal{R}(\emptyset) = \emptyset$, and $\mathcal{R}(\{a\}) = \{a, b, c\}$. In this case we see that the conflict-freeness requirement in Lemma 4.3(c) is sufficient but not necessary, since $\{a, b, c\}$ is *not* conflict-free, but nevertheless $\mathcal{R}(\{a\}) = \mathcal{R}(\mathcal{R}(\{a\})) = \{a, b, c\}$.
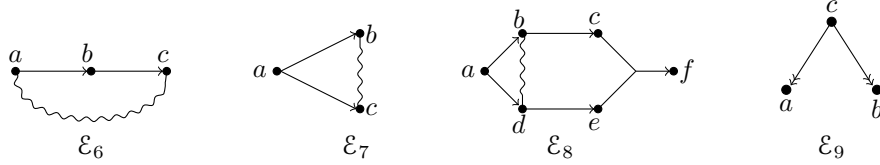
Figure 2.   Four CES.

(3) In $\mathcal{E}_8$, we have that $\mathcal{R}(\{a\}) = \{a, b, c, d, e\}$ is *not* conflict-free. Then, Lemma 4.3(c) does not apply and in fact $\mathcal{R}(\{a\} \cup \{c, e\}) = \{a, b, c, d, e, f\} \supsetneq \mathcal{R}(\{a\})$.

For conflict-free CES, we can inductively characterize the reachable events. This is done in Def. 4.5 in the form of inference rules.

Definition 4.5. For all $X \subseteq E$, we inductively define the set $\hat{\mathcal{R}}(X)$ as follows:

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

Recall that, by saturation of $\vdash$ and by Notation 2.3, the premise $\hat{\mathcal{R}}(X) \vdash e$ in rule $\vdash_{\hat{\mathcal{R}}}$ actually means that there exists a *finite* set of events $e_1, \ldots, e_n \in \hat{\mathcal{R}}(X)$ such that $\{e_1, \ldots, e_n\} \vdash e$ (similarly for $\Vdash_{\hat{\mathcal{R}}}$). More pedantically, rule $\vdash_{\hat{\mathcal{R}}}$ actually stands for the set of rules:

$$\frac{e_1 \in \hat{\mathcal{R}}(X) \quad \cdots \quad e_n \in \hat{\mathcal{R}}(X)}{e \in \hat{\mathcal{R}}(X)} \quad \text{if } \{e_1, \ldots, e_n\} \vdash e$$

Example 4.6. Let us consider the CES $\mathcal{E}_2$ of Fig.1. We have the following derivation:

$$\cfrac{b \Vdash a \qquad \cfrac{a \vdash b \qquad \cfrac{\cfrac{\overline{a \in \{a\}}}{a \in \hat{\mathcal{R}}(\{a\})}(\in_{\hat{\mathcal{R}}})}{b \in \hat{\mathcal{R}}(\{a\})}(\vdash_{\hat{\mathcal{R}}})}{a \in \hat{\mathcal{R}}(\emptyset)}}{}(\Vdash_{\hat{\mathcal{R}}})$$

Furthermore, since $a \in \hat{\mathcal{R}}(\emptyset)$, from rule $\vdash_{\hat{\mathcal{R}}}$ we also obtain $b \in \hat{\mathcal{R}}(\emptyset)$.

The inductive characterization of reachable events coincides with Def. 4.1, for conflict-free CES.

Theorem 4.7. For all CES $\mathcal{E}$, and for all $X \subseteq E$, $\mathcal{R}_{\mathcal{E}}(X) \subseteq \hat{\mathcal{R}}_{\mathcal{E}}(X)$, Moreover, if $\mathcal{E}$ is conflict-free, then $\mathcal{R}_{\mathcal{E}}(X) \supseteq \hat{\mathcal{R}}_{\mathcal{E}}(X)$.

Notice that, in the presence of conflicts, $\mathcal{R}_{\mathcal{E}}(X)$ could be *strictly* contained in $\hat{\mathcal{R}}_{\mathcal{E}}(X)$. For instance, in the ES $\mathcal{E}_8$ in Fig. 2, the event f is *not* reachable, but it belongs to $\hat{\mathcal{R}}(\emptyset)$. Indeed, the events c and e (which cause f) are both reachable, but they cannot appear together in a configuration.

We now give an alternative characterization of reachable events for finite conflict-free CES. This reformulation (Theorem 4.8) yields a polynomial-time algorithm for computing the set $\mathcal{R}$ (whereas computing them through the inference rules of Def. 4.5 would give an exponential algorithm). The algorithm exploits Kleene's fixed point theorem, by defining the set $\mathcal{R}$ as the greatest fixed point of a monotonic (increasing) function F, defined below.

Theorem 4.8. For all $X, Y, Z \subseteq E$, let:

$$G_Y(Z) = Y \cup \{e \mid Z \vdash e\}$$
$$F(X) = \mathrm{lfp}\, G_{\{e \mid X \Vdash e\}}$$

Then, for all finite conflict-free CES $\mathcal{E}$, we have $\mathcal{R}_{\mathcal{E}} = \mathrm{gfp}\, F$

Following the characterization provided by Theorem 4.8, an algorithm for constructing $\mathcal{R}_{\mathcal{E}}$ can be devised as follows. Let X_0 be the set of all events in $\mathcal{E}$. At step 0, we compute $X_1 = F(X_0)$. This can be done by interpreting the (minimal) $\vdash$-enablings of $\mathcal{E}$ as a set of propositional Horn clauses, and then by applying the forward chaining algorithm with input $\{e \mid X_0 \Vdash e\}$. The forward chaining can be computed in polynomial-time in the number of $\vdash$-enablings. If $X_1 = X_0$, then we have finished, i.e. $X_1 = \mathcal{R}_{\mathcal{E}}$. Otherwise, we compute $X_2 = F(X_1)$ and so on, until reaching a fixed point. In the worst case, this requires $|E|$ steps, hence we have a polynomial-time algorithm for computing $\mathcal{R}_{\mathcal{E}}$.

5. An LTS semantics of CES

In this section we define an operational semantics of CES. This is given in terms of a Labelled Transition System (LTS), the states of which are pairs (C, X). The first element of such pair is the set of events occurred so far; the second element is a set of events taken "on credit". Intuitively, in all the reachable states (C, X), C is an X-configuration and X is minimal for C.

We will first observe what happens when adding an event e to a trace $\sigma \in \mathcal{T}(X)$. It is always true that $\sigma e \in \mathcal{T}(X \cup \{e\})$, although $X \cup \{e\}$ may *not* be the least credit for σe. Def. 5.1 below establishes how the credits of a trace change when adding an event. When Def. 5.1 is instantiated with $C = \overline{\sigma}$ and X is the least credit of σ, then Lemma 5.3 guarantees that $\Delta(C, X, e)$ is the least credit for σe. Intuitively, in Def. 5.1 we first remove from X the set of credits which have been honoured by performing e; then, we add e unless it is justified.

Definition 5.1. For all $C, X \subseteq E$ and for all $e \in E$, we define:

$$\Delta(C, X, e) = (X \setminus \{x \in X \mid C \cup \{e\} \Vdash x\}) \cup \begin{cases} \{e\} & \text{if } C \cup \{e\} \not\Vdash e \wedge C \not\vdash e \\ \emptyset & \text{otherwise} \end{cases}$$

Example 5.2. Recall the CES $\mathcal{E}_2$ from Fig. 1. The trace $\langle a \rangle$ belongs to $\mathcal{T}(\{a\})$, and $\{a\}$ is its least credit. Of course $\langle a\, b \rangle \in \mathcal{T}(\{a, b\})$, but since b is $\vdash$-enabled by $\{a\}$, it is not necessary to take b on credit. Moreover, since $b \Vdash a$, we can also remove a from the credit set: hence $\langle a\, b \rangle \in \mathcal{T}$. Indeed, the least credit for $\langle a\, b \rangle$ is computed through Def. 5.1 as $\Delta(\{a\}, \{a\}, b) = (\{a\} \setminus \{a\}) \cup \emptyset = \emptyset$.

Lemma 5.3. Let $\sigma = \sigma' e$, with $e \notin \overline{\sigma'}$ and $CF(\overline{\sigma})$. If $\sigma' \in \mathcal{T}(X)$, then $\sigma \in \mathcal{T}(\Delta(\overline{\sigma'}, X, e))$. Moreover, if X is the least credit for σ', then $\Delta(\overline{\sigma'}, X, e)$ is the least credit for σ.

As noticed in Ex. 5.2, adding events to a trace may reduce the credit set. Also, observe that changing the order in which events are performed may change the credit set. In particular when an event without $\Vdash$-enablings is fired before its $\vdash$-justification, it will not be possible to remove it from the credit set by firing new events. For instance, if in Ex. 5.2 we fire b before a, then we cannot remove b from the credit set. This allows for correctly recording the events performed in the absence of a causal justification.

Example 5.4. Consider the CES $\mathcal{E}_9$ in Fig. 2. The trace $\langle ab \rangle$ has least credit $\{a, b\}$; by adding the event c, the least credit for $\langle abc \rangle$ becomes $\{c\}$.

Definition 5.5. (LTS)
For all CES $\mathcal{E}$, we define the labelled transition system $\mathrm{LTS}_{\mathcal{E}} = \langle S, E, \rightarrow_{\mathcal{E}} \rangle$, where $S = Con \times Con$, and the relation $\rightarrow_{\mathcal{E}}$ is defined as follows:

$$\frac{e \notin C \qquad CF(C \cup \{e\})}{(C, X) \xrightarrow{e}_{\mathcal{E}} (C \cup \{e\}, \Delta(C, X, e))}$$

We say that (C, X) is a reachable state of $\mathrm{LTS}_{\mathcal{E}}$ iff $(\emptyset, \emptyset) \rightarrow_{\mathcal{E}}^* (C, X)$. When clear from the context, we will omit the index $\mathcal{E}$ from $\rightarrow_{\mathcal{E}}$.

We remark that if $\mathcal{E}$ has no circular enablings, then $\mathrm{LTS}_{\mathcal{E}}$ can be characterised in a simpler form, i.e. $(C, X) \xrightarrow{e} (C \cup \{e\}, X)$ if $C \vdash e$, and $(C, X) \xrightarrow{e} (C \cup \{e\}, X \cup \{e\})$ if $C \nvdash e$. The subrelation of $\rightarrow_{\mathcal{E}}$ containing only states with empty credits coincides with the transition relation defined in [21].

By Def. 5.5 it immediately follows that, for all CES $\mathcal{E}$, the relation $\rightarrow_{\mathcal{E}}$ is *deterministic*, i.e. whenever $(C, X) \xrightarrow{a} (C', X')$ and $(C, X) \xrightarrow{a} (C'', X'')$, it must be $(C', X') = (C'', X'')$. Determinism is a very desirable property, e.g. in the context of contracts, because it ensures that the events to be performed by a participant at any given time are uniquely determined by the past actions.

Two immediate consequences of Def. 5.5 are reported in Lemma 5.6 below. In item (a) we start from a state (C, X), from which we fire a sequence of events σ. Then, we reach a state (C', X') where C' exactly comprises all the events in $C \cup \overline{\sigma}$, and the events which are removed from the credits are circularly enabled by the events in $C \cup \overline{\sigma}$. Item (b) states that the set X in a state $(\overline{\sigma}, X)$ is the least credit for σ — and so $X \subseteq \overline{\sigma}$ for all reachable states $(\overline{\sigma}, X)$. Notice that there may exist different reachable states (C, X) with same the same C and uncomparable X. This is because, in general, there exists no least credit for a set of events C.

Lemma 5.6. For all $C, C', X, X' \subseteq E$, and for all $\sigma \in E^*$:

(a) $(C, X) \xrightarrow{\sigma} (C', X') \implies \overline{\sigma} = C' \setminus C \ \wedge \ C \cup \overline{\sigma} \Vdash X \setminus X'$

(b) $\sigma \in \mathcal{T}(X) \ \wedge \ X$ least credit for $\sigma \iff (\emptyset, \emptyset) \xrightarrow{\sigma} (\overline{\sigma}, X)$

Example 5.7. Recall the CES $\mathcal{E}_2$ from Fig. 1 (its enablings are $a \vdash b$ and $b \Vdash a$). According to its LTS (depicted in Fig. 3, left), in the initial state we can fire either the event a or the event b, by taking it on credit. In the state $(\{a\}, \{a\})$ we can perform the event b, and reach the state $(\{a, b\}, \emptyset)$. Instead, when performing a in the state $(\{b\}, \{b\})$ we reach the state $(\{a, b\}, \{b\})$. The event b cannot be discharged from that credit set, since there does not exists any $\Vdash$-enabling for it.
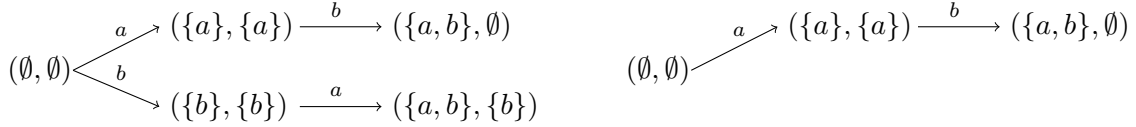
Figure 3.   The LTS of CES $\mathcal{E}_2$ (left), and its urgent LTS (right).

The following theorem relates configurations with reachable states of the LTS. A (possibly infinite) set C is an X-configuration iff for all finite subsets D of C there exists a state with events containing D and with credits contained in X.

Theorem 5.8. For all CES $\mathcal{E}$, and for all $C, X \subseteq E$:

$$C \in \mathcal{F}(X) \iff \forall D \subseteq_{fin} C, \exists X_0 \subseteq_{fin} X. \exists C_0. \ D \subseteq C_0 \subseteq C. \ (\emptyset, \emptyset) \to^* (C_0, X_0)$$

The LTS of a CES also gives an alternative way to characterise the reachable events.

Lemma 5.9. For all CES $\mathcal{E}$, for all $e \in E$, and for all $X \subseteq E$:

$$e \in \mathcal{R}(X) \iff \exists C_0 \subseteq E, X_0 \subseteq_{fin} X. \ (\emptyset, \emptyset) \to^* (C_0, X_0) \ \wedge \ e \in C_0$$

Computations on $\mathrm{LTS}_{\mathcal{E}}$ are far too liberal: they allow us to fire an event either if it is ($\vdash$ or $\Vdash$)-enabled by the already fired events, or — by taking it on credit — if it will be honoured in the future, or even if it will not. Except for the conflicting events, any event can be fired, with the risk of keeping such event in the credit set forever. Intuitively, one would like to perform those events only which allow to eventually reach a state with empty credits. Such events will be called *urgent*.

Definition 5.10. (Urgent events)
For all $e \in E$, and for all $C, X \subseteq E$, we say that e is *urgent* in (C, X) iff

$$\exists \sigma. \ (C, X) \xrightarrow{e\sigma}_{\mathcal{E}} (C \cup \overline{e\sigma}, \emptyset)$$

We denote with $\mathcal{U}_{\mathcal{E}}^C(X)$ the set of urgent events in (C, X).

Intuitively, the events that are urgent in (C, X) are those already enabled by C, or those which can be done on credit, on behalf that they will be honoured when the right choices will be made in the future. For instance, in $\mathcal{E}_2$ the event a is urgent in the initial state $(\emptyset, \emptyset)$. In such state b is *not* urgent, but it will be urgent in the state $(\{a\}, \{a\})$ where a has been performed on credit.

Note that the definition of urgent events implicitly considers non-deterministic choices as *angelic*, modelling a situation where a set of participants (the entities which fire events) *cooperate* to reach a common goal. Indeed, an urgent event guarantees the existence of a trace leading to an empty credit set, and such behavior intuitively is the one that will be followed in a cooperative setting. In other words, angelic non-determinism guarantees that only the choices which lead to the goal are taken.

The case of *demonic* non-determinism, modelling a situation where participants *compete* to reach their (possibly conflicting) goals, is quite more complex.

For instance, assume we extend $\mathcal{E}_2$ with the enabling $a \vdash c$ and the conflict $b \# c$. Then, Def. 5.10 states that a is urgent in the initial state. Indeed, assume that a is fired in the initial state; then, one has the choice to perform either b or c. In a cooperative setting, only the branch b can be taken, because it is the only way to reach an honoured trace. Instead, in a competitive setting (i.e. with demonic non-determinism), the event a should *not* be considered urgent, because an adversary could choose the branch c, and then prevent from reaching an honoured trace.

In the competitive setting, one could be tempted to define urgent events by just requiring that *all* the choices lead to an honoured trace. However, this definition would be too strict, because it does not take into account the fact that each participant can always control her own choices. A definition of urgent events in competitive settings has been proposed in [5], by setting up a suitable game-theoretic model.

Example 5.11. Consider $\mathcal{E}_2$ and its LTS depicted in Fig. 3: a is urgent in $(\emptyset, \emptyset)$, because there exists a path from $(\{a\}, \{a\})$ which leads to an empty credit set. For the same reason, b is urgent in $(\{a\}, \{a\})$. On the contrary b is *not* urgent in $(\emptyset, \emptyset)$, because whatever choices are made in the future, it would not be possible to honour the credit $\{b\}$. Indeed, if a transition labelled b is taken from state $(\emptyset, \emptyset)$ of $\mathrm{LTS}_{\mathcal{E}_2}$, then all future states will contain the credit b.

Pruning away from an LTS all the transitions labelled by non-urgent events, we obtain a new LTS, denoted by $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$. The crucial property of the $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$ is that, by following its transitions, one is always guaranteed to reach a state where all the credits have been honoured (see Lemma 5.14 below). For instance, Fig. 3 (right) displays the urgent LTS for $\mathcal{E}_2$.

Definition 5.12. We define the relation $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$ as the largest subset of $\rightarrow_\mathcal{E}$ such that:

$$(C, X) \xrightarrow{e}_{\mathcal{U}_\mathcal{E}} (C', X') \qquad \text{iff } (C, X) \xrightarrow{e}_\mathcal{E} (C', X') \text{ and } e \in \mathcal{U}^C(X)$$

Note that in the absence of circularity the LTS $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$ coincides with the LTS defined in [21], where the component X is always empty. For instance, let us consider an event structure without circular enablings, and let (C, X) be a reachable state in its LTS. If $X \neq \emptyset$, then the credit X will never be honoured since there are no circular enablings, hence no events will be urgent in (C, X). Otherwise, if $X = \emptyset$, then the urgent events in $(C, \emptyset)$ are exactly those events e such that $C \vdash e$. This is because, by Def. 5.5, $(C, \emptyset) \xrightarrow{e} (C \cup \{e\}, \emptyset)$ if $C \vdash e$.

The following lemma relates the traces in $\mathcal{T}_\mathcal{E}$ with the traces in $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$. The traces in $\mathcal{T}_\mathcal{E}$ are exactly those traces in $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$ which lead to a state (C, X) with $X = \emptyset$.

Lemma 5.13. For all σ:

$$\sigma \in \mathcal{T}_\mathcal{E} \iff (\emptyset, \emptyset) \xrightarrow{\sigma}_{\mathcal{U}_\mathcal{E}} (\overline{\sigma}, \emptyset)$$

The following lemma establishes a crucial property of the LTS $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$, that is the ability to reach, starting from any state (C, X) reachable from $(\emptyset, \emptyset)$ and following only $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$ transitions, a state where all the credits have been honoured.

Lemma 5.14. Let (C, X) be a reachable state of $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$. Then, $\exists \eta. (C, X) \xrightarrow{\eta}_{\mathcal{U}_\mathcal{E}} (C \cup \overline{\eta}, \emptyset)$

The following lemma relates urgent events with reachability: reachable events in $\mathcal{E}$ are exactly those events which label some transition in the LTS $\twoheadrightarrow_{\mathcal{U}_\mathcal{E}}$.
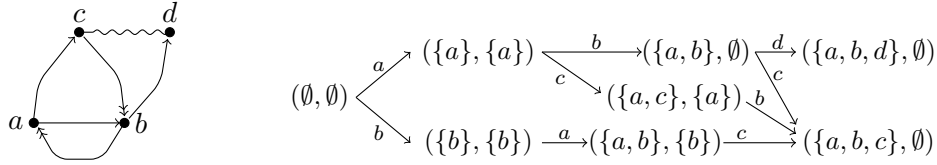
Figure 4. An event structure $\mathcal{E}$ (left) and the LTS $\rightharpoonup_{\mathcal{U}_\mathcal{E}}$ (right).

Lemma 5.15. For all CES $\mathcal{E}$, and for all $C, X \subseteq E$:

$$\mathcal{R}_\mathcal{E} \;=\; \{e \mid \exists \sigma : (\emptyset, \emptyset) \xrightarrow{\sigma}_{\mathcal{U}_\mathcal{E}} \xrightarrow{e}_{\mathcal{U}_\mathcal{E}}\}$$

A relevant question is whether, for any CES $\mathcal{E}$, there exists a CES $\mathcal{E}'$ without circular enablings such that the LTS $\rightharpoonup_{\mathcal{U}_\mathcal{E}}$ equals to $\rightarrow_{\mathcal{E}'}$. In other words, we wonder whether the expressiveness with the urgent LTS is the same as that of the LTS of Winskel's ES. A negative answer is displayed in Fig. 4, which shows a CES $\mathcal{E}$ for which there exists no ES the LTS of which corresponds to $\rightharpoonup_{\mathcal{U}_\mathcal{E}}$. Indeed, ES cannot distinguish between two states which only differ for the credits, like e.g. $(\{a, b\}, \emptyset)$ and $(\{a, b\}, \{b\})$ in Fig. 4. In Winskel's ES, a transition from a state C only depends on the events in C, and not on the order in which these events have been fired. Instead, transitions in CES also depend on the credits accumulated in the history of execution.

In the case of conflict-free CES, we provide in Def. 5.16 an alternative characterisation of urgent events. Unlike $\mathcal{U}^C(X)$, the set $\hat{\mathcal{U}}^C(X)$ also contains all the events in C. The relation between $\mathcal{U}^C(X)$ and $\hat{\mathcal{U}}^C(X)$ is formalised in Lemma 5.17 below.

Definition 5.16. For all $C, X \subseteq E$, we define the set $\hat{\mathcal{U}}^C(X)$ as follows:

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

Lemma 5.17. For a a conflict-free CES $\mathcal{E}$, and a reachable state (C, X) of $\rightharpoonup_{\mathcal{U}_\mathcal{E}}$:

$$\hat{\mathcal{U}}^C_\mathcal{E}(X) \;=\; \mathcal{U}^C_\mathcal{E}(X) \cup C$$

Note that the definition of urgent events (Def. 5.10) is declarative. In concrete applications of CES, when a participant has to decide which event to fire, it would be desirable to also have an algorithmic description. In the case of finite CES, it is possible to find the set of urgent events by model checking the LTS of the CES against the reachability property required by Def. 5.10. For finite conflict-free CES, an algorithm for constructing the urgent events $\mathcal{U}^C$ in a state (C, X) is obtained as follows. By Lemma 5.17, $\mathcal{U}^C(X) = \hat{\mathcal{U}}^C(X) \setminus C$. The set $\hat{\mathcal{U}}^C(X)$ is constructed by direct application of the three rules in Def. 5.16, where the set $\mathcal{R}(C \cup X)$ in the premise of rule $(\Vdash_{\hat{u}})$ is computed through the polynomial-time algorithm provided by Theorem 4.8. For the more general setting of infinite CES, we come up against the problem of undecidability, yet algorithmic results can be obtained by considering suitable subclasses of CES (e.g. model checking temporal logic on finite representations of infinite ES, as in [15]).

6. Relations with logics

In this section we investigate some relations between CES and logics. In particular, we shall consider Propositional Contract Logic (PCL, [7]), which allows for circular reasoning. We first shortly review PCL, and then in sections 6.1 and 6.2 we shall discuss our main results.

PCL extends intuitionistic propositional logic (IPC) with a new binary connective, called *contractual implication* and denoted by $\twoheadrightarrow$. Differently from IPC, a formula $p \twoheadrightarrow q$ implies q not only when p is provable, but also in the case that a "compatible" formula holds. 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. PCL has been used as a contract model in a calculus for contracting processes [7], and it has been related to a communication-based contract model in [6]. We assume a denumerable set $a, b, \ldots$ of prime (atomic) formulae. PCL formulae are denoted with the letters $p, q, r, s, \ldots.$.

Definition 6.1. The formulae of PCL are defined as:

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

A proof system for PCL is provided in [7], both in terms of an Hilbert-style and a Gentzen-style axiomatisation (which are shown in [7] to be equivalent). Here we only consider the Gentzen-style proof system, which extends the rules for IPC presented in [16] with the following three rules (the full rule set is reported in Appendix C):

$$\frac{\begin{array}{c}\Gamma, \, p \twoheadrightarrow q, \, r \; \vdash \; p \\ \Gamma, \, p \twoheadrightarrow q, \, q \; \vdash \; r\end{array}}{\Gamma, \, p \twoheadrightarrow q \vdash r} \text{ (Fix)} \qquad \frac{\Gamma \vdash q}{\Gamma \vdash p \twoheadrightarrow q} \text{ (Zero)} \qquad \frac{\begin{array}{c}\Gamma, \, p \twoheadrightarrow q, \, a \; \vdash \; p \\ \Gamma, \, p \twoheadrightarrow q, \, q \; \vdash \; b\end{array}}{\Gamma, \, p \twoheadrightarrow q \vdash a \twoheadrightarrow b} \text{ (PrePost)}$$

Rule Fix is the left rule for $\twoheadrightarrow$. It is almost the same as the left rule for $\to$, except that (in a "circular" fashion) the formula r can be used to deduce p in the first rule premise. Rule Zero introduces $\twoheadrightarrow$ on the right of a sequent (similarly e.g. to $\bigcirc R$ of lax logic [10]), while rule PrePost introduces $\twoheadrightarrow$ on the right, and eliminates it on the left (similarly e.g. to $\bigcirc L$ of [10]).

The main result of [7] is the decidability of the entailment relation $\vdash$, which is a direct consequence of the cut elimination and subformula properties enjoyed by the proof system.

A first correspondence between CES and PCL can be observed by comparing the three items of Lemma 3.9 with the rules Cut, $\to$L and Fix of PCL, respectively:

$$\frac{C \in \mathcal{F}(X) \quad C' \in \mathcal{F}(X \cup C)}{C \cup C' \in \mathcal{F}(X)} \text{ (3.9(a))} \qquad \frac{\Gamma \vdash p \quad \Gamma, p \vdash q}{\Gamma \vdash q} \text{ (Cut)}$$

$$\frac{C \in \mathcal{F}(X) \quad C' \in \mathcal{F}(X \cup Y) \quad C \vdash Y}{C \cup C' \in \mathcal{F}(X)} \text{ (3.9(b))} \qquad \frac{\Gamma \vdash p \quad \Gamma, q \vdash r \quad p \to q \in \Gamma}{\Gamma \vdash r} \text{ ($\to$L)}$$

$$\frac{C \in \mathcal{F}(X \cup C') \quad C' \in \mathcal{F}(X \cup Y) \quad C \Vdash Y}{C \cup C' \in \mathcal{F}(X)} \text{ (3.9(c))} \qquad \frac{\Gamma, r \vdash p \quad \Gamma, q \vdash r \quad p \twoheadrightarrow q \in \Gamma}{\Gamma \vdash r} \text{ (Fix)}$$

Notice that, under the hypotheses of Lemma 3.9, the stronger thesis $C' \in \mathcal{F}(X)$ does not hold in general. For instance, consider the CES with enablings $a \Vdash b$, $b \Vdash a$, $a \vdash c$. We have that $C = \{a, b\} \in \mathcal{F}$ and $C' = \{a, c\} \in \mathcal{F}(C)$. By Lemma 3.9(a), it then follows that $C \cup C' \in \mathcal{F}$, but C' alone is not a configuration. Similar examples hold for items (b) and (c).

6.1. Reachability via logic

In Def. 6.2 we show a translation from CES into PCL formulae. In particular, our mapping is a bijection of finite, conflict-free CES into the Horn fragment of PCL, which comprises atoms, conjunctions and non-nested (standard/contractual) implications. To disambiguate the enabling $\vdash$ of CES from the entailment relation of PCL, below we shall denote the latter with $\vdash_{\mathrm{PCL}}$. Also, when writing $X \vdash e$ we shall mean that X is a minimal set of events such that $(X, e) \in \vdash$ (similarly for $\Vdash$).

The encoding $[\cdot]_{\mathcal{R}}$ maps an enabling $\vdash$ into an $\rightarrow$-clause, and a circular enabling $\Vdash$ into an $\twoheadrightarrow$-clause.

Definition 6.2. Let $\mathcal{E} = \langle E, \#, \vdash, \Vdash \rangle$ be a conflict-free CES. The mapping $[\cdot]_{\mathcal{R}}$ from $\mathcal{E}$ into sets of PCL formulae is defined as follows:

$$[(X_i \circ e_i)_{i \in I}]_{\mathcal{R}} = \{[X_i \circ e_i]_{\mathcal{R}} \mid i \in I\} \qquad \textit{where } [\circ] = \begin{cases} \rightarrow & \text{if } \circ = \vdash \\ \twoheadrightarrow & \text{if } \circ = \Vdash \end{cases}$$

$$[X \circ e]_{\mathcal{R}} = \left(\bigwedge X\right) [\circ] e$$

Notice that the encoding above can be inverted, i.e. one can also translate a Horn PCL theory into a conflict-free CES. Indeed, the encoding can be seen as an isomorphism.

For each event $e \in E$, we assume an atom e in PCL. For a conjunction of atoms $\varphi = \bigwedge_{i \in I} e_i$, we write $\overline{\varphi}$ for the set $\{e_i \mid i \in I\}$. We extend this notation to sets Φ of conjunctions of atoms: we write $\overline{\Phi}$ for $\bigcup\{\overline{\varphi} \mid \varphi \in \Phi\}$, and Φ, Φ' for $\Phi \cup \Phi'$.

Lemma 6.3. Let $\mathcal{E}$ be a finite, conflict-free CES. For all φ and Φ, $\overline{\varphi} \subseteq \mathcal{R}_{\mathcal{E}}(\overline{\Phi})$ iff $[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash_{\mathrm{PCL}} \varphi$.

A direct consequence of the above lemma (by choosing $\varphi = e$ and $\Phi = \emptyset$) is the correctness and completeness of the encoding.

Theorem 6.4. Let $\mathcal{E}$ be a finite, conflict-free CES. For all $e \in E$, we have $e \in \mathcal{R}_{\mathcal{E}}$ iff $[\mathcal{E}]_{\mathcal{R}} \vdash_{\mathrm{PCL}} e$.

Theorem 6.4 has two important consequences. First, together with Theorem 4.8, it provides us with a polynomial-time algorithm for checking provability in Horn PCL theories (in contrast with the fact that provability in full PCL is PSPACE-hard, as well as in IPC and in its implicational fragment [19]). Second, we can exploit properties of PCL to derive properties of conflict-free CES. For instance, from the tautology $(a \rightarrow b) \wedge (b \twoheadrightarrow c) \rightarrow (a \twoheadrightarrow c)$ of PCL we deduce that any conflict-free CES with enablings $a \vdash b$ and $b \Vdash c$ can be enriched with the enabling $a \Vdash c$, without affecting the reachable events.

6.2. Configurations via logic

We now show that the problem of deciding if a set of events is a configuration in a CES can be reduced to provability in the logic PCL (which is shown in [7] to be decidable).

Note that, even in the case where $\mathcal{E}$ is conflict-free, one cannot simply exploit the encoding $[\mathcal{E}]_{\mathcal{R}}$ in Def. 6.2 to test whether a set of events C is a configuration or not. A wrong attempt would be to check

the entailment $[\mathcal{E}]_\mathfrak{R} \vdash_{\text{PCL}} C$. This would be incorrect, because, in general, not every set of reachable events is a configuration. For instance, in the CES $\mathcal{E}_2$ in Ex. 2.5(2) the set $\{a, b\}$ is a configuration, but $\{a\}$ and $\{b\}$ are not.

To test if a set C is a configuration, besides requiring that C only contains reachable events, we also have to ensure that any event in C can be justified by using only other events in C. To do that, we first tag with ! the events in C, and then we encode each enabling similarly to Def. 6.2, but guaranteeing that an event can be proved only if all its justifications belong to C. For instance, $a \Vdash b$ is encoded as the clause $(!a \land !b \land a) \twoheadrightarrow b$, from which we can deduce b only if both a and b belong to the set C.

Technically, for a CES $\mathcal{E} = \langle E, \#, \vdash, \Vdash \rangle$ and a set $X \subseteq E$, we denote with $!X$ the set $\{!e \mid e \in X\}$. We assume $!E$ disjoint from E, i.e. $!E \cap E = \emptyset$. For a set $X \subseteq E \cup !E$, we define $X^\flat = X \cap E$, and $X^! = \{e \in E \mid !e \in X\}$. According to this notation, for all sets of atoms $X, Y \subseteq E \cup !E$, we have (i) $X = X^\flat \cup !(X^!)$, and (ii) if $X \subseteq Y$, then $X^\flat \subseteq Y^\flat$ and $X^! \subseteq Y^!$.

Definition 6.5. Let $\mathcal{E} = \langle E, \#, \vdash, \Vdash \rangle$ be a CES. The mapping $[\cdot]_\mathfrak{F}$ from $\mathcal{E}$ into sets of PCL formulae is defined as follows:

$$[(X_i \circ e_i)_{i \in I}]_\mathfrak{F} \;\;=\;\; \{[X_i \circ e_i]_\mathfrak{F} \mid i \in I\}$$

$$[X \circ e]_\mathfrak{F} \;\;=\;\; (!e \land X \land !X)[\circ]\,e \qquad where\,[\circ] = \begin{cases} \to & \text{if } \circ = \vdash \\ \twoheadrightarrow & \text{if } \circ = \Vdash \end{cases}$$

$$[a \# b]_\mathfrak{F} \;\;=\;\; (!a \land !b) \to \bot$$

Intuitively, we want to test if a set of events C is an X-configuration. To do that, we first tag with a ! all the events in C, and then assume $\Gamma = [\mathcal{E}]_\mathfrak{F}, !C, X$. The encoding $[\cdot]_\mathfrak{F}$ maps a conflict $a \# b$ to a formula $(!a \land !b) \to \bot$. Therefore, if C is *not* conflict-free then its encoding will deduce $\bot$. Otherwise, we check if C is entailed by Γ. The encoding of $\mathcal{E}$ will be a set of clauses of the form $(!e \land X \land !X)[\circ]\,e$. The $!e$ on the left of the clause ensures that e can be proved only if it belongs to C. Similarly, the $!X$ ensures that the justifications of e belong to C as well.

Lemma 6.6 establishes two basic properties of the encoding. Item (a) states that if a !-atom is provable, then it must already be present in Φ (i.e. it cannot be generated by the encoding). Item (b) states that, under the hypothesis $\overline{\Phi}^\flat \subseteq \overline{\Phi}^!$, if an atom e without ! is provable, then $!e$ must belong to Φ. Intuitively, this is caused by the fact that the encoding requires $!e$ on the left of all clauses which produce e.

Lemma 6.6. For all sets of conjunctions of atoms Φ, and for all conjunctions of atoms φ such that $[\mathcal{E}]_\mathfrak{F}, \Phi \vdash_{\text{PCL}} \varphi$ and $[\mathcal{E}]_\mathfrak{F}, \Phi \not\vdash_{\text{PCL}} \bot$, we have (a) $\overline{\varphi}^! \subseteq \overline{\Phi}^!$, and (b) $\overline{\Phi}^\flat \subseteq \overline{\Phi}^! \implies \overline{\varphi}^\flat \subseteq \overline{\Phi}^!$

The following theorem gives a criterion to decide if C is an X-configuration.

Theorem 6.7. Let $\mathcal{E}$ be a finite CES. For all $C \subseteq E$ and for all $X \subseteq E$:

$$C \in \mathcal{F}_\mathcal{E}(X) \quad \Longleftrightarrow \quad [\mathcal{E}]_\mathfrak{F}, !C, X \vdash_{\text{PCL}} C \text{ and } [\mathcal{E}]_\mathfrak{F}, !C, X \not\vdash_{\text{PCL}} \bot$$

Example 6.8. Recall the CES $\mathcal{E}_3$ from Fig. 1. We have that:

$$[\mathcal{E}_3] = \{ (!c \land !a \land !b \land a \land b) \to c, \;\; (!a \land !c \land c) \twoheadrightarrow a, \;\; (!b \land !c \land c) \twoheadrightarrow b \}$$

Let $C = \{a, b, c\}$. We have that $C \in \mathcal{F}_{\mathcal{E}_3}$, and $[\mathcal{E}_3]$, $!C \vdash_{\text{PCL}} C$. Note that, were the !-ed atoms omitted in the premises of $\to / \twoheadrightarrow$, then we would have, *e.g.*, $[\mathcal{E}_3]$, $!a$, $!c \vdash_{\text{PCL}} a \wedge c$, from which by Theorem 6.7 we would have incorrectly deduced that $\{a, c\} \in \mathcal{F}_{\mathcal{E}_3}$.

7. Related work and conclusions

We have extended Winskel's event structures with a new enabling relation, which allows for reasoning about circular dependencies among events which are part of the same configuration. To the best of our knowledge, beside some approaches we will discuss below, the other event-based models appeared in the literature do not consider circular dependencies in the same way as we do. Circularity may exist in the relations among events (as in Boudol's flow event structures [8]) but these relations, when restricted to the events in a configuration, give a partial order, whereas in our case this is not true.

Observe that our notion of configuration (Def. 2.4) assumes the axiom of finite causes, i.e. it requires that every event in a configuration has a *finite* justification, both in the past (through both kinds of enablings), and in the future (through $\Vdash$-enablings). An interesting variant of our theory can be obtained by dropping the axiom of finite causes on the events taken on credit. Consider e.g. the CES:

$$e_0 \leftarrowtail e_1 \leftarrowtail e_2 \leftarrowtail e_3 \leftarrowtail e_4 \leftarrowtail \cdots$$

it might be arguable whether the set $C = \{e_i \mid i \geq 0\}$ has to be considered a configuration or not. For instance, if the CES models an ever-growing debit (similarly to the money-lender scenario of Example 2.7) the borrower would reasonably *not* consider C as a successful execution of the system. Indeed, Def. 2.4 rules out C as a configuration, because, for all i, there exists no *finite* trace containing e_i (hence the only configuration there is the empty one).

In some scenarios, the ability of honouring a debt "at the limit" could be acceptable. To drop the axiom of finite causes on the events taken on credit, we should also allow for *infinite* traces, e.g. $\langle e_0\, e_1 \ldots \rangle$ in the example above. This modification would make the set C above a configuration, at the cost of losing the finiteness property (Def. 3.11), and all the properties deriving from it (e.g. Lemma 3.3). Furthermore, because of the presence of infinite chains of $\Vdash$-enablings, the rules defining reachable events for conflict-free CES (Def. 4.5) must be interpreted coinductively, by allowing for infinite derivations. Note that not all infinite derivations are acceptable, e.g. an infinite path of rules $\vdash_{\hat{\mathcal{R}}}$ would violate the axiom of finite causes for $\vdash$-enablings. We conjecture that reachable events are those for which there exists a derivation where each infinite path contains an infinite number of occurrences of rule $\Vdash_{\hat{\mathcal{R}}}$.

Circular reasoning often appears in the compositional modelling and verification of systems. Circularity issues have been investigated in assume-guarantee reasoning [1, 2, 13, 20], in models of workflow systems [11], in logic programming [18, 17]. Circularity is also a common situation when reasoning about contracts [7, 5, 4]: circular dependencies arise when two or more tasks mutually rely on the guarantees provided by each other. We briefly discuss some of these approaches below.

In [11] a generalization of prime event structures is proposed where a *response* relation (denoted with $\bullet\to$) is used to characterise the accepting traces as those where, for each $a \bullet\to b$, if a is present in the trace, then b eventually occurs after a. The response relation bears some resemblance with our $\Vdash$ relation, but there are some notable differences. First, having $a \Vdash b$ does not necessarily imply that a configuration containing a must also contain b (another enabling could have been used), whereas $a \bullet\to b$ stipulates that once one has a in a configuration, then also b must be present. Indeed, an enabling $a \Vdash b$

can be neglected, whereas $a \bullet\!\!\to b$ must be used. Also, augmenting the number of $\Vdash$-enablings increases the number of configurations, while adding more response relations reduces it.

Circularity is dealt with at a logical (proof-theoretic) level in [7]. The Horn fragment of PCL is strongly related to finite CES: in particular, provability of atoms corresponds to reachability of events in conflict-free CES (Theorem 6.4); configurations can be reduced as well to provability and consistency checking of PCL formulae (Theorem 6.7).

The motivations underlying the circular enabling of CES seem related to those introduced in [2] to compose assume-guarantee specifications [1]. There, the idea is that 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 [2], this is rendered as 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, the validity of this judgment (not valid in IPC) is subject to a side condition on the interpretation of M_1, M_2 in the model. In our approach we obtain a similar goal through the circular enabling: the CES with enablings $m_1 \Vdash m_2$ and $m_2 \Vdash m_1$ has $\{m_1, m_2\}$ as a configuration.

The issue of circular dependencies among events has been addressed also in the Petri nets' world. In [4] a notion of *lending* Petri nets (LPNs) has been introduced. In LPNs places are partitioned into two sets: lending places and normal ones. A transition may be executed even if some of the lending places in the preset are not marked, thus *borrowing* tokens from such places. A successful computation in an LPN is a computation where all the borrowed tokens are given back. LPNs with some additional constraints, *contract nets*, have been then developed as a concrete counterpart of logical contracts specified as Horn PCL formulae. A correspondence between CES and contract nets can be established. Successful computations in a contract net correspond to configurations in the associated CES and *vice versa*. Indeed, borrowing tokens in contract nets is similar to firing events on credit. However in a CES events may be taken on credit without any restriction, whereas this is not possible in contract net, hence computations in contract nets are somehow less liberal than in CES. We also conjecture that urgent actions in LPNs, i.e. those actions which preserve the ability to reach an honoured marking, correspond to urgent events in the associated CES.

In coinductive logic programming (CLP, [17]), both coinduction and induction can be used to give semantics to programs, i.e. to sets of Horn clauses. Intuitively, this can be related to CES in that $\vdash$ has an inductive flavour, while $\Vdash$ a coinductive one. However, two main differences exist between the two frameworks. First, in CLP all the clauses for the same predicate have to share their inductive/coinductive nature. That is, there is no equivalent for $a_1 \vdash b$, $a_2 \Vdash b$ because b is used in both fashions. Second, CLP forbids circular dependencies between inductive and coinductive predicates, requiring stratification. For instance, CLP allows for expressing $a \Vdash b$, $b \Vdash a$, as well as $a \vdash b$, $b \Vdash c$, while it forbids $a \vdash b$, $b \Vdash a$ because b would be inductive while a would be coinductive. Other approaches mixing induction and coinduction (e.g. [12]) work under a similar stratification assumption. We believe that by assuming stratification one can find good connections between CES and CLP. However, we think that (unconstrained) circularity is an essential feature of concurrent systems, and in particular of contracts. For instance, the system $a \vdash b$, $b \Vdash a$ is an archetypal scenario in contracting systems, where we are both expressing circularity between a and b, and a legitimate ordering between the events, i.e. a must occur before b. In CES, we can encompass both aspects: in the above example, $\{a, b\}$ is a configuration, and the LTS of urgent events describes the traces which respect the causal ordering imposed by $\vdash$-enablings (while $\Vdash$ does not prescribe any order). Therefore, requiring stratification in CES would seem to trivialize them. Note in passing that PCL requires no stratification, hence it can be meaningfully related to CES.

References

[1] Abadi, M., Lamport, L.: Composing Specifications, *ACM Transactions on Programming Languages and Systems*, **15**(1), 1993.

[2] Abadi, M., Plotkin, G. D.: A Logical View of Composition, *Theoretical Computer Science*, **114**(1), 1993.

[3] Baldan, P., Corradini, A., Montanari, U.: Contextual Petri Nets, Asymmetric Event Structures, and Processes, *Inf. Comput.*, **171**(1), 2001, 1–49.

[4] Bartoletti, M., Cimoli, T., Pinna, G. M.: Lending Petri nets and contracts, *Proc. FSEN*, 2013, To appear.

[5] Bartoletti, M., Cimoli, T., Zunino, R.: A theory of agreements and protection, *Proc. POST*, 2013, To appear.

[6] Bartoletti, M., Tuosto, E., Zunino, R.: Contract-oriented Computing in CO_2 , *Scientific Annals in Computer Science*, **22**(1), 2012, 5–60.

[7] Bartoletti, M., Zunino, R.: A Calculus of Contracting Processes, *LICS*, 2010.

[8] Boudol, G.: Flow Event Structures and Flow Nets, *Semantics of Systems of Concurrent Processes*, 469, Springer, 1990.

[9] Cimoli, T.: *A theory of agreements and protection*, Ph.D. Thesis, Dipartimento di Matematica e Informatica, University of Cagliari, 2013.

[10] Fairtlough, M., Mendler, M.: Propositional Lax Logic, *Information and Computation*, **137**(1), 1997.

[11] Hildebrandt, T. T., Mukkamala, R. R.: Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs, *Proc. PLACES*, 69, 2010.

[12] Leroy, X., Grall, H.: Coinductive big-step operational semantics, *Inf. Comput.*, **207**(2), 2009, 284–304.

[13] Maier, P.: Compositional Circular Assume-Guarantee Rules Cannot Be Sound and Complete, *Proc. FoSSaCS*, 2003.

[14] Nielsen, M., Plotkin, G. D., Winskel, G.: Petri Nets, Event Structures and Domains, Part I, *Theor. Comput. Sci.*, **13**, 1981, 85–108.

[15] Penczek, W.: Model-Checking for a Subclass of Event Structures, *Proc. TACAS*, 1217, Springer, 1997.

[16] Pfenning, F.: Structural Cut Elimination - I. Intuitionistic and Classical Logic, *Information and Computation*, **157**(1/2), 2000, 84–141.

[17] Simon, L., Bansal, A., Mallya, A., Gupta, G.: Co-Logic Programming: Extending Logic Programming with Coinduction, *Proc. ICALP*, 2007.

[18] Simon, L., Mallya, A., Bansal, A., Gupta, G.: Coinductive Logic Programming, in: *Logic Programming*, Springer, 2006, 330–345.

[19] Statman, R.: Intuitionistic propositional logic is polynomial-space complete, *Theoretical Computer Science*, **9**, 1979, 67–72.

[20] Viswanathan, M., Viswanathan, R.: Foundations for Circular Compositional Reasoning, *ICALP*, 2001.

[21] Winskel, G.: Event Structures, *Advances in Petri Nets*, 1986.

[22] Winskel, G.: An Introduction to Event Structures, *REX Workshop*, 1988.

A. Proofs for Section 4

Definition A.1. Let the predicate $DF(\sigma)$ be true iff σ has no duplicates, i.e. $DF(\sigma) \equiv \forall i \leq n : e_i \notin \overline{\sigma_i}$.

Proof of Lemma 4.3:
For (a), let $e \in X$. Since $CF(\{e\})$, by Lemma 3.7(3.7) it follows that $\{e\} \in \mathcal{F}(\{e\})$. By Lemma 3.7(3.7), we also have $\{e\} \in \mathcal{F}(X)$. Thus, by Def. 4.1 it follows that $e \in \mathcal{R}(X)$.

For (b), let e in $\mathcal{R}(X)$. By Def. 4.1, there exists $C \in \mathcal{F}(X)$ such that $e \in C$. Since $X \subseteq Y$, by Lemma 3.7(3.7) we also have $C \in \mathcal{F}(Y)$. Hence, $e \in \mathcal{R}(Y)$.

For (c), the inclusion $\subseteq$ follows directly by item (b). For the inclusion $\supseteq$, let $e \in \mathcal{R}(C \cup X)$, and let $C = \{e_i\}_i \subseteq \mathcal{R}(X)$. By Def. 4.1, there exists $C' \in \mathcal{F}(C \cup X)$ such that $e \in C'$, and for all events $e_i \in C$, there exists $C_i \in \mathcal{F}(X)$ such that $e_i \in C_i$. Let $\mathcal{A} = \{C_i \mid e_i \in C\}$, and let $C_j, C_k \in \mathcal{A}$. By Def. 4.1, $C_j, C_k \subseteq \mathcal{R}(X)$. Since $CF(\mathcal{R}(X))$ follows by hypothesis, then $CF(C_j \cup C_k)$, and so by Theorem 3.12, $C_j \cup C_k \in \mathcal{F}(X)$. Thus, by Def. 3.10, the family of X-configurations $\mathcal{A}$ is pairwise compatible. By Theorem 3.12, $F = \bigcup \mathcal{A} \in \mathcal{F}(X)$. Since $F \subseteq \mathcal{R}(X)$ and $C' \subseteq \mathcal{R}(C \cup X)$, then $F \cup C' \subseteq \mathcal{R}(C \cup X)$, and thus $CF(F \cup C')$ follows by the premise of (c). By Lemma 3.7(3.7), since $C' \in \mathcal{F}(C \cup X)$ and $C \subseteq F$, then $C' \in \mathcal{F}(F \cup X)$. Therefore, by Lemma 3.9(a), $e \in F \cup C' \in \mathcal{F}(X)$, and so $e \in \mathcal{R}(X)$. $\qquad\square$

In Lemma A.2 we summarise some basic properties of the operator $\hat{\mathcal{R}}$: similarly to $\mathcal{R}$, it is monotonic; and we have that $\hat{\mathcal{R}}(X)$ is a fix point of $\hat{\mathcal{R}}$. Finally in Lemma 4.7 we prove that $\mathcal{R}$ and $\hat{\mathcal{R}}$ are equal.

Lemma A.2. For all $X, Y \subseteq E$:

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

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

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

Proof:
Item (a) is straightforward by rule $(\in_{\hat{\mathcal{R}}})$. Item (b) is by easy induction on the depth of the derivation of $e \in \hat{\mathcal{R}}(X)$. For item (c), the inclusion $\hat{\mathcal{R}}(X) \subseteq \hat{\mathcal{R}}(\hat{\mathcal{R}}(X))$ follows by item (a). The other inclusion can be easily proved by induction on the depth of the proof of $e \in \hat{\mathcal{R}}(\hat{\mathcal{R}}(X))$. $\qquad\square$

Lemma A.3. For all $X, Y \subseteq E$, $Y \subseteq \hat{\mathcal{R}}(X) \implies \hat{\mathcal{R}}(X \cup Y) = \hat{\mathcal{R}}(X)$.

Proof:
The inclusion $\hat{\mathcal{R}}(X \cup Y) \supseteq \hat{\mathcal{R}}(X)$ follows directly by Lemma A.2(b). For the other inclusion, by Lemma A.2(b) and A.2(c) we have:

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

By Lemma A.2(a), $Y \subseteq \hat{\mathcal{R}}(Y)$. Since $\hat{\mathcal{R}}(Y) \subseteq \hat{\mathcal{R}}(X)$, then by Lemma A.2(b) we have $\hat{\mathcal{R}}(X \cup Y) \subseteq \hat{\mathcal{R}}(X \cup \hat{\mathcal{R}}(X))$. By Lemma A.2(a), $X \subseteq \hat{\mathcal{R}}(X)$, and so $\hat{\mathcal{R}}(X \cup \hat{\mathcal{R}}(X)) = \hat{\mathcal{R}}(\hat{\mathcal{R}}(X))$. By Lemma A.2(c), we have $\hat{\mathcal{R}}(\hat{\mathcal{R}}(X)) = \hat{\mathcal{R}}(X)$, which concludes. $\qquad\square$

Lemma A.4. For all $X \subseteq E, Y \subseteq_{fin} E, \ \hat{\mathcal{R}}(X \cup Y) \Vdash Y \implies Y \subseteq \hat{\mathcal{R}}(X)$.

Proof:
If $Y = \emptyset$, the statement holds trivially. Otherwise, let $Y = \{e_0, \ldots, e_k\}$. For all $i \leq k$, we define $Y_i = \{e_0, \ldots, e_i\}$, and $Y^i = Y \setminus Y_i = \{e_{i+1}, \ldots, e_k\}$. We shall prove that:

$$\forall i \leq k. \ Y_i \subseteq \hat{\mathcal{R}}(X \cup Y^i) \tag{3}$$

To prove (3), we proceed by mathematical induction.

- Base case $i = 0$.

  By hypothesis, $\hat{\mathcal{R}}(X \cup Y) \Vdash e_0$. Then:

  $$\frac{\hat{\mathcal{R}}(X \cup Y) \Vdash e_0}{e_0 \in \hat{\mathcal{R}}((X \cup Y) \setminus \{e_0\})} \ (\Vdash_{\hat{\mathcal{R}}})$$

  So we have proved that $\{e_0\} = Y_0 \subseteq \hat{\mathcal{R}}((X \cup Y) \setminus \{e_0\}) \subseteq \hat{\mathcal{R}}(X \cup Y^0)$.

- Inductive case. By the induction hypothesis, we have that $Y_i \subseteq \hat{\mathcal{R}}(X \cup Y^i)$. By Lemma A.3, $\hat{\mathcal{R}}(X \cup Y^i \cup Y_i) = \hat{\mathcal{R}}(X \cup Y^i)$. By $(\in_{\mathcal{R}})$, we have $e_{i+1} \in \hat{\mathcal{R}}(X \cup Y) = \hat{\mathcal{R}}(X \cup Y^i \cup Y_i) = \hat{\mathcal{R}}(X \cup Y^i)$. By hypothesis, $\hat{\mathcal{R}}(X \cup Y^i \cup Y_i) \Vdash e_{i+1}$, and so $\hat{\mathcal{R}}(X \cup Y^i) \Vdash e_{i+1}$. Hence we can apply rule $(\Vdash_{\hat{\mathcal{R}}})$ to obtain:

  $$\frac{\hat{\mathcal{R}}(X \cup Y^i) \Vdash e_{i+1}}{e_{i+1} \in \hat{\mathcal{R}}(X \cup Y^{i+1})} \ (\Vdash_{\hat{\mathcal{R}}}) \tag{4}$$

  We obtain the thesis of (3) as follows:

  $$\begin{aligned}
  Y_{i+1} &= Y_i \cup \{e_{i+1}\} && \text{(by Def. } Y_i) \\
  &\subseteq \hat{\mathcal{R}}(X \cup Y^i) \cup \{e_{i+1}\} && \text{(by the induction hypothesis)} \\
  &= \hat{\mathcal{R}}(X \cup Y^i) && \text{(by } e_{i+1} \in \hat{\mathcal{R}}(X \cup Y^i)) \\
  &= \hat{\mathcal{R}}(X \cup Y^{i+1} \cup \{e_{i+1}\}) && \text{(by Def. } Y^i) \\
  &= \hat{\mathcal{R}}(X \cup Y^{i+1}) && \text{(by Lemma A.3 and (4))}
  \end{aligned}$$

Back to the main statement, just note that for $i = k$ in (3), we obtain the thesis $Y = Y_k \subseteq \hat{\mathcal{R}}(X)$. $\qquad \square$

In Def. A.5 below we define how the credit set of a trace changes when removing the last event (see [9] for a more detailed account of this topic). When the set X in Def. A.5 is the least credit of σ, then Lemma A.6 will guarantee that $\Delta^-(\sigma, X, e)$ is the least credit of σe. Differently from Def. 5.1, we need a trace instead of a configuration, since we need to know the order in which events have been done.

Definition A.5. For all $X \subseteq E$, for all $\sigma = \langle e_0 \ldots e_n \rangle$, and for all $e \in E$, we define:

$$\Delta^-(\sigma, X, e) \ = \ (X \setminus \{e\}) \ \cup \ \{e_i \in \overline{\sigma} \mid \overline{\sigma e} \Vdash e_i \ \wedge \ \overline{\sigma} \not\Vdash e_i \ \wedge \ \overline{\sigma_i} \not\vdash e_i\} \tag{5}$$

Lemma A.6. Let $\sigma = \sigma'e = \langle e_0 \dots e_n \rangle$, with $e_n = e$. Then,

$$\sigma \in \mathcal{T}(X) \implies \sigma' \in \mathcal{T}(\Delta^-(\sigma', X, e))$$

Moreover, if X is the least credit for σ', then $\Delta^-(\sigma', X, e)$ is least credit for σ.

Proof:
Let $\sigma = \sigma'e = \langle e_0 \dots e_n \rangle \in \mathcal{T}(X)$, with $e_n = e$. Since $\sigma \in \mathcal{T}(X)$, by eq. (1) we have that:

$$CF(\overline{\sigma}) \ \wedge \ DF(\sigma) \ \wedge \ \forall i \le n. \ (e_i \in X \ \vee \ \overline{\sigma_i} \vdash e_i \ \vee \ \overline{\sigma} \Vdash e_i)$$

Since σ' is a prefix of σ then $CF(\overline{\sigma'})$ and $DF(\sigma')$. Moreover, e only occurs in the last position, hence:

$$\forall i \le n - 1. \ (e_i \in (X \setminus \{e\}) \ \vee \ \overline{\sigma'_i} \vdash e_i \ \vee \ \overline{\sigma} \Vdash e_i) \ \wedge \ (e \in X \ \vee \ \overline{\sigma'} \vdash e \ \vee \ \overline{\sigma} \Vdash e) \quad (6)$$

Let us define the set D as:

$$D \ = \ \{e_i \in \overline{\sigma'} \mid \overline{\sigma} \Vdash e_i \ \wedge \ \overline{\sigma'} \not\Vdash e_i \ \wedge \ \overline{\sigma'_i} \not\vdash e_i\} \quad (7)$$

We will prove that $\sigma' \in \mathcal{T}(R)$, with $R = (X \setminus \{e\}) \cup D$. Let $i \le n - 1$. By (6), we have three cases:

- $e_i \in X$. Since $e_i \ne e$ for all $i < n$, then $e_i \in X \setminus \{e\} \subseteq R$.

- $\overline{\sigma_i} \vdash e_i$. Since σ' is a prefix of σ, for all $i < n$ it holds that $\overline{\sigma'_i} \vdash e_i$.

- $\overline{\sigma_i} \not\vdash e_i$ and $\overline{\sigma} \Vdash e_i$. If $\overline{\sigma'} \Vdash e_i$, then e_i is justified in σ'. Otherwise, we have $e_i \in D \subseteq R$.

We have then proved that $\sigma' \in \mathcal{T}(R)$.

We now prove that R is a minimal credit for σ'. By contradiction, assume that there exists some $Y \subset R$ such that $\sigma' \in \mathcal{T}(Y)$. Pick an $e_i \in \overline{\sigma'}$ such that $e_i \in R \setminus Y$. By hypothesis, $\sigma' \in \mathcal{T}(Y)$, so it must be:

$$\overline{\sigma'_i} \vdash e_i \ \vee \ \overline{\sigma'} \Vdash e_i$$

We have two cases:

- $\overline{\sigma'_i} \vdash e_i$. Since $e_i \in R \setminus Y$, we have two cases: $e_i \in X \setminus \{e\}$ or $e_i \in D$. Note that by (7), it cannot be $e_i \in D$. If $e_i \in X \setminus \{e\}$, then we would have $\sigma \in \mathcal{T}(X \setminus \{e_i\})$, which contradicts the hypothesis that X is a minimal credit for σ.

- $\overline{\sigma'} \Vdash e_i$. As above we have two cases: $e_i \in X \setminus \{e\}$ or $e_i \in D$. Note that by (7), it cannot be $e_i \in D$. If $e_i \in X \setminus \{e\}$, then we would have $\sigma \in \mathcal{T}(X \setminus \{e_i\})$, which contradicts the hypothesis that X is a minimal credit for σ.

In both cases we have a contradiction; thus R is a minimal credit for σ, and by Lemma 3.5, A is a least credit. □

Lemma A.7. For all $C, X \subseteq E, \ C \in \mathcal{F}(X) \implies C \subseteq \hat{\mathcal{R}}(X)$.

Proof:
We will first prove that $\forall C_0 \subseteq_{fin} C. \; \forall X. \; C_0 \in \mathcal{F}(X) \implies C_0 \subseteq \hat{\mathcal{R}}(X)$. Let $C_0 \subseteq_{fin} C$, and assume that $C_0 \in \mathcal{F}(X)$, for some X. By Corollary 3.4 we have that:

$$\exists \sigma = \langle e_0 \dots e_n \rangle \in \mathcal{T}(X). \; \overline{\sigma} = C_0$$

We proceed by induction on the size of C_0. In the base case $C_0 = \emptyset$ the thesis holds trivially. For the inductive case, let us assume $C_0 \neq \emptyset$. Let $e_n = e$, let $\sigma' = \langle e_0 \dots e_{n-1} \rangle$ and let $C' = \overline{\sigma'}$. We will prove that $C' \subseteq \hat{\mathcal{R}}(X)$ and $e \subseteq \hat{\mathcal{R}}(X)$. Let:

$$D \;\; = \;\; \{ e_i \in \overline{\sigma'} \mid \overline{\sigma} \Vdash e_i \;\; \wedge \;\; \overline{\sigma'} \not\Vdash e_i \;\; \wedge \;\; \overline{\sigma_i'} \not\vdash e_i \} \tag{8}$$

By Lemma A.6, $\sigma' \in \mathcal{T}(X \cup D)$. By Lemma 3.4, $C' \in \mathcal{F}(X \cup D)$, and then by the induction hypothesis, $C' \subseteq \hat{\mathcal{R}}(X \cup D)$. Now, we will prove that $e \in \hat{\mathcal{R}}(X \cup D)$. Since $e = e_n \in \overline{\sigma}$, by eq. (1), to justify e in σ we must have:

$$e \in X \;\; \vee \;\; \overline{\sigma'} \vdash e \;\; \vee \;\; \overline{\sigma} \Vdash e$$

We have the following three cases:

- if $e \in X$, by $(\in_{\hat{\mathcal{R}}})$ we have that $e \in \hat{\mathcal{R}}(X)$ and by Lemma 3.7(3.7), $e \in \hat{\mathcal{R}}(X \cup D)$.

- if $\overline{\sigma'} \vdash e$, since by the induction hypothesis $C' \subseteq \hat{\mathcal{R}}(X \cup D)$ and $C' \vdash e$, then by saturation $\hat{\mathcal{R}}(X \cup D) \vdash e$. Therefore by $(\vdash_{\hat{\mathcal{R}}})$ we have:

$$\frac{\hat{\mathcal{R}}(X \cup D) \vdash e}{e \in \hat{\mathcal{R}}(X \cup D)} \; (\vdash_{\hat{\mathcal{R}}})$$

- if $\overline{\sigma} \Vdash e$, since by the induction hypothesis $C' \subseteq \hat{\mathcal{R}}(X \cup D)$, then by Lemma 3.7(3.7), $C_0 = C' \cup \{e\} \subseteq \hat{\mathcal{R}}(X \cup D \cup \{e\})$. By saturation, $\overline{\sigma} = C_0 \Vdash e$ implies $\hat{\mathcal{R}}(X \cup D \cup \{e\}) \Vdash e$. Therefore, by $(\Vdash_{\hat{\mathcal{R}}})$ we have:

$$\frac{\hat{\mathcal{R}}(X \cup D \cup \{e\}) \Vdash e}{e \in \hat{\mathcal{R}}(X \cup D)} \; (\Vdash_{\hat{\mathcal{R}}})$$

So we have proved that $e \in \hat{\mathcal{R}}(X \cup D)$, hence $C_0 = C' \cup \{e\} \subseteq \hat{\mathcal{R}}(X \cup D)$. Note that by (8), we have that $C_0 \Vdash D$, and so by saturation $\hat{\mathcal{R}}(X \cup D) \Vdash D$. Therefore by Lemma A.4, $D \subseteq \hat{\mathcal{R}}(X)$. By Lemma A.3, it follows that $\hat{\mathcal{R}}(X \cup D) = \hat{\mathcal{R}}(X)$, and the thesis follows because $C_0 \subseteq \hat{\mathcal{R}}(X \cup D)$.

Back to the main statement, since $C \in \mathcal{F}(X)$ we have that for all $e \in C$, there exists $\sigma^e \in \mathcal{T}(X)$ such that $e \in \overline{\sigma^e} \subseteq_{fin} C$. Since $\overline{\sigma^e} \in \mathcal{F}(X)$, we have proved above that $\overline{\sigma^e} \subseteq \hat{\mathcal{R}}(X)$. Therefore, $C = \bigcup \{ \overline{\sigma^e} \mid e \in C \} \subseteq \hat{\mathcal{R}}(X)$. $\qquad\qquad\square$

Proof of Theorem 4.7:
($\subseteq$) Let $e \in \mathcal{R}(X)$. By Def. 4.1, there exists a configuration $C \in \mathcal{F}(X)$ such that $e \in C$. By Lemma A.7, $e \in C \subseteq \hat{\mathcal{R}}(X)$.

($\supseteq$) Assume that $e \in \hat{\mathcal{R}}(X)$. We will prove that $\exists C \in \mathcal{F}(X)$ such that $e \in C$. By Def. 4.1, this will allow to conclude $e \in \mathcal{R}(X)$. We proceed by induction on the depth of the derivation of $e \in \hat{\mathcal{R}}(X)$. According to the last rule used in the derivation, we have the following three cases:

- case $(\in_{\hat{\mathcal{R}}})$. We have that

$$\frac{e \in X}{e \in \hat{\mathcal{R}}(X)} \ (\in_{\hat{\mathcal{R}}})$$

Since $e \in X$, by Lemma 3.7 we have that $e \in \{e\} \in \mathcal{F}(X)$.

- case $(\vdash_{\hat{\mathcal{R}}})$.

$$\frac{\hat{\mathcal{R}}(X) \vdash e}{e \in \hat{\mathcal{R}}(X)} \ (\vdash_{\hat{\mathcal{R}}})$$

The premise $\hat{\mathcal{R}}(X) \vdash e$ implies that there exists $D \subseteq_{fin} \hat{\mathcal{R}}(X)$ such that $D \vdash e$. By the induction hypothesis, for all $d \in D$ there exists $C_d \in \mathcal{F}(X)$ such that $d \in C_d$. Let $C = \bigcup_{d \in D} C_d$. Since $\mathcal{E}$ is conflict-free, by Theorem 3.12 it follows that $C \in \mathcal{F}(X)$. Since $D \subseteq C$ and $D \vdash e$, by saturation we have $C \vdash e$. By Lemma 3.7(3.7), $\{e\} \in \mathcal{F}(\{e\})$. Therefore, by Lemma 3.9(b), $C \cup \{e\} \in \mathcal{F}(X)$.

- case $[\Vdash_{\hat{\mathcal{R}}}]$

$$\frac{\hat{\mathcal{R}}(X \cup \{e\}) \Vdash e}{e \in \hat{\mathcal{R}}(X)} \ [\Vdash_{\hat{\mathcal{R}}}]$$

The premise $\hat{\mathcal{R}}(X \cup \{e\}) \Vdash e$ implies that there exists $D \subseteq_{fin} \hat{\mathcal{R}}(X \cup \{e\})$ such that $D \Vdash e$. By the induction hypothesis, for all $d \in D$ there exists $C_d \in \mathcal{F}(X \cup \{e\})$ such that $d \in C_d$. Let $C = \bigcup_{d \in D} C_d$. Since $\mathcal{E}$ is conflict-free, by Theorem 3.12 it follows that $C \in \mathcal{F}(X \cup \{e\})$. By Lemma 3.7(3.7), $\{e\} \in \mathcal{F}(X \cup \{e\})$. Since $D \subseteq C$ and $D \Vdash e$, by saturation we have $C \Vdash e$. Therefore, Lemma 3.9(c) gives that $C \cup \{e\} \in \mathcal{F}(X)$.

$\square$

Proof of Theorem 4.8:
The function G_X is monotonic. Since the domain is finite, it is also continuous, hence by Kleene's fixed point theorem, $\mathrm{lfp}\, G_X = \bigcup_{i \in \omega} G_X^i(\emptyset)$. Similarly, F is monotonic, and so it is continuous and also co-continuous.

We first show that $\mathcal{R} \subseteq \mathrm{gfp}\, F$. By Tarski's fixed point theorem, $\mathrm{gfp}\, F$ is the least upper bound of the post-fixed points of F, i.e. of the sets X for which $X \subseteq F(X)$. Therefore, to obtain the thesis it suffices to prove that $\mathcal{R} \subseteq F(\mathcal{R})$. By Def. 4.1, we have that $\mathcal{R} = \bigcup \{\overline{\sigma} \mid \sigma \in \mathcal{T}\}$. It then suffices to show that $\overline{\sigma} \subseteq F(\mathcal{R})$, for all $\sigma \in \mathcal{T}$. We proceed by induction on the length of the sequence σ:

- base case: $\sigma = \langle\rangle$. The thesis follows trivially.

- inductive case: $\sigma = \eta\, e$. By the induction hypothesis, $\overline{\eta} \subseteq F(\mathcal{R})$. We have two further subcases, according on how e has been justified in the trace.

  - If $\overline{\eta} \vdash e$, then since $\overline{\eta} \subseteq F(\mathcal{R})$, by saturation of $\vdash$ it follows that $F(\mathcal{R}) \vdash e$. By definition of G, it follows that $e \in G_X(F(\mathcal{R}))$, for all X. In particular, $e \in G_{\{e' \mid \mathcal{R} \Vdash e'\}}(F(\mathcal{R}))$, which is equal to $F(\mathcal{R})$ by definition of F.

  - If $\overline{\sigma} \Vdash e$, then since $\overline{\sigma} \subseteq \mathcal{R}$, by saturation of $\Vdash$ it follows that $\mathcal{R} \Vdash e$. Thus, we conclude that $e \in \{e' \mid \mathcal{R} \Vdash e'\} \subseteq \mathrm{lfp}\, G_{\{e' \mid \mathcal{R} \Vdash e'\}} = F(\mathcal{R})$.

We now show that gfp $F \subseteq \mathcal{R}$. To do that, consider an arbitrary fixed point Y of F, i.e. assume that $Y = F(Y)$. We will prove that $Y \subseteq \mathcal{R}$, which gives the thesis. Let $K = \{e \mid Y \Vdash e\}$. Since $Y = F(Y)$, then by Kleene's fixed point theorem we have $Y = \text{lfp} \, G_K = \bigcup_{i \in \omega} G_K^i(\emptyset)$. We will now construct a sequence $\sigma \in \mathcal{T}$ such that $\overline{\sigma} = Y$. Since $\mathcal{E}$ is finite, the chain:

$$\emptyset = G_K^0(\emptyset) \subseteq G_K^1(\emptyset) \subseteq G_K^2(\emptyset) \subseteq \cdots \subseteq G_K^i(\emptyset) \subseteq \cdots$$

stabilizes to $\text{lfp} \, G_K$ after a finite number (say, n) of steps. We then construct a sequence $\sigma = \sigma^1 \sigma^2 \cdots \sigma^n$ as follows. Each σ^i is an arbitrary ordering of the events in the sets Y_i, defined as:

$$Y_i = G_K^i(\emptyset) \setminus \left(\bigcup_{j<i} Y_j \right)$$

We have that:

$$
\begin{aligned}
G_K^1(\emptyset) &= K \cup \{e \mid \emptyset \vdash e\} & Y_1 &= K \cup \{e \mid \emptyset \vdash e\} \\
G_K^2(\emptyset) &= K \cup \{e \mid Y_1 \vdash e\} & Y_2 &= \{e \mid Y_1 \vdash e\} \setminus Y_1 \\
G_K^3(\emptyset) &= K \cup \{e \mid Y_1 \cup Y_2 \vdash e\} & Y_3 &= \{e \mid Y_1 \cup Y_2 \vdash e\} \setminus (Y_1 \cup Y_2) \\
&\cdots & &\cdots \\
G_K^i(\emptyset) &= K \cup \{e \mid \bigcup_{j<i} Y_j \vdash e\} & Y_i &= \{e \mid \bigcup_{j<i} Y_j \vdash e\} \setminus (\bigcup_{j<i} Y_j)
\end{aligned}
$$

Therefore, for all $i > 0$, $(\bigcup_{j<i} Y_j) \vdash Y_i \setminus K$.

We show that σ is a trace of $\mathcal{E}$. For each event e occurring in σ, there exists $i \leq n$ such that $e \in \overline{\sigma^i}$. One of the following two cases applies:

- $i = 1$. Then, either $e \in K$, or $\emptyset \vdash e$. In the first case, e has a justification in σ because $Y \Vdash e$ (by definition of K) and $Y = \overline{\sigma}$. In the second case, e is trivially justified.

- $i > 1$. Since $(\bigcup_{j<i} Y_j) \vdash Y_i$, then e is justified by the events in $\sigma^1 \cdots \sigma^{i-1}$.

Therefore, $\sigma \in \mathcal{T}$, and so by Def. 4.1, $\overline{\sigma} \subseteq \mathcal{R}$. By construction we have $\overline{\sigma} = Y$, hence $Y \subseteq \mathcal{R}$. Since Y is an arbitrary fixed point of F, then *a fortiori* we conclude that gfp $F \subseteq \mathcal{R}$. $\qquad \square$

B. Proofs for Section 5

Proof of Lemma 5.3:
Let $\sigma' = \langle e_0 \ldots e_n \rangle \in \mathcal{T}(X')$, let $\sigma = \sigma' e$, and let $X = \Delta(\overline{\sigma'}, X', e)$. By equation (1) it is easy to see that $\sigma \in \mathcal{T}(X)$. Let X' be the least credit for σ'. We prove that X is the least credit for σ. By Def. 5.3:

$$X = \Delta(\overline{\sigma'}, X', e) = (X' \setminus \{x \in X' \mid \overline{\sigma'} \cup \{e\} \Vdash x\}) \cup \begin{cases} \{e\} & \text{if } \overline{\sigma'} \cup \{e\} \not\Vdash e \wedge \overline{\sigma'} \not\vdash e \\ \emptyset & \text{otherwise} \end{cases}$$

By Lemma 3.5, $X' = \{e_i \in \overline{\sigma'} \mid \overline{\sigma'_i} \not\vdash e_i \wedge \overline{\sigma'} \not\Vdash e_i\}$. Since $\overline{\sigma'} \cup \{e\} = \overline{\sigma}$, we have:

$$X = (\{e_i \in \overline{\sigma'} \mid \overline{\sigma'_i} \not\vdash e_i \wedge \overline{\sigma'} \not\Vdash e_i\} \setminus \{x \in X' \mid \overline{\sigma} \Vdash x\}) \cup \begin{cases} \{e\} & \text{if } \overline{\sigma} \not\Vdash e \wedge \overline{\sigma'} \not\vdash e \\ \emptyset & \text{otherwise} \end{cases}$$

Since X' is the least credit for σ', we have that $X' \subseteq \overline{\sigma'}$. Hence:

$$X \;=\; (\{e_i \in \overline{\sigma'} \mid \overline{\sigma'_i} \not\Vdash e_i \;\wedge\; \overline{\sigma} \not\Vdash e_i\}) \;\cup\; \begin{cases} \{e\} & \text{if } \overline{\sigma} \not\Vdash e \;\wedge\; \overline{\sigma'} \not\Vdash e \\ \emptyset & \text{otherwise} \end{cases}$$

By renaming e as e_{n+1}, we have $\sigma = \langle e_0 \dots e_n e_{n+1} \rangle$, hence

$$X = (\{e_i \in \overline{\sigma} \mid \overline{\sigma_i} \not\Vdash e_i \;\wedge\; \overline{\sigma} \not\Vdash e_i\}$$

By Lemma 3.5, X is the least credit for σ. $\qquad\square$

Proof of Lemma 5.6:

Item (a) is straightforward by Def. 5.5.

For item (b$\Rightarrow$), let $\sigma \in \mathcal{T}(X)$. By induction on the length of $\sigma = \langle e_0 \dots e_n \rangle$, we prove that for all $i \leq n$, if Y_i is the least credit for σ_i, then $(\emptyset, \emptyset) \xrightarrow{\sigma_i} (\overline{\sigma_i}, Y_i)$. The base case is trivial, since the least credit for $\sigma_0 = \varepsilon$ is $Y_0 = \emptyset$. For the inductive case, by the induction hypothesis assume that $(\emptyset, \emptyset) \xrightarrow{\sigma_i} (\overline{\sigma_i}, Y_i)$. Then, by Def. 5.5:

$$(\overline{\sigma_i}, Y_i) \xrightarrow{e_i} (\overline{\sigma_{i+1}}, \Delta(\overline{\sigma_i}, Y_i, e_i))$$

By Lemma 5.3, $\Delta(\overline{\sigma_i}, Y_i, e_i) = Y_{i+1}$ is the least credit for σ_{i+1}.

For (b$\Leftarrow$), by an easy inductive argument on the length of σ (using Lemma 5.3 at each step) it follows that, for all $i \leq n$, if $(\emptyset, \emptyset) \xrightarrow{\sigma_i} (\overline{\sigma_i}, Y_i)$, then Y_i is the least credit for $\overline{\sigma_i}$. This implies $\sigma \in \mathcal{T}(X)$. $\qquad\square$

Proof of Theorem 5.8:

($\Rightarrow$) Let $C \in \mathcal{F}(X)$, and let $D \subseteq_{fin} C$. By Lemma 3.3, there exists $\sigma \in \mathcal{T}(X)$ such that $D \subseteq \overline{\sigma} \subseteq C$. Let $X_0 \subseteq_{fin} X$ be the least credit for σ. By Lemma 5.6, we have $(\emptyset, \emptyset) \xrightarrow{\sigma} (\overline{\sigma}, X_0)$. Therefore, the thesis follows by choosing $C_0 = \overline{\sigma}$.

($\Leftarrow$) Let $D \subseteq_{fin} C$, and assume that $(\emptyset, \emptyset) \xrightarrow{\sigma} (C_0, X_0)$, for some σ and X_0 such that $C_0 = \overline{\sigma}$, $D \subseteq C_0 \subseteq C$, and $X_0 \subseteq X$. Assume that $\sigma = \langle e_0 \dots e_n \rangle$, and that the trace has the form:

$$(\emptyset, \emptyset) \xrightarrow{e_0} (\overline{\sigma_1}, Y_1) \xrightarrow{e_1} (\overline{\sigma_2}, Y_2) \xrightarrow{e_2} \cdots \xrightarrow{e_n} (\overline{\sigma}, Y_n)$$

where $Y_n = X_0$. By Lemma 5.6(b), we have $\sigma \in \mathcal{T}(X_0)$. Since $X_0 \subseteq_{fin} X$, by Lemma 3.2(b), it is also true that $\sigma \in \mathcal{T}(X)$. Therefore, by Lemma 3.3 we conclude that $C \in \mathcal{F}(X)$. $\qquad\square$

Proof of Lemma 5.9:

($\Rightarrow$) Let $e \in \mathcal{R}(X)$. By Def. 4.1, there exists $C \in \mathcal{F}(X)$ such that $e \in C$. Since $C \in \mathcal{F}(X)$, by Theorem 5.8 there exists $X_0 \subseteq_{fin} X$ and C_0 such that $(\emptyset, \emptyset) \rightarrow^* (C_0, X_0)$ and $e \in C_0 \subseteq_{fin} C$.

($\Leftarrow$) Let σ be such that $(\emptyset, \emptyset) \xrightarrow{\sigma} (C_0, X_0)$, with $e \in C_0$ and $X_0 \subseteq_{fin} X$. By Lemma 5.6(b), $\sigma \in \mathcal{T}(X_0)$. Thus, $e \in \overline{\sigma} \in \mathcal{F}(X_0)$. By Lemma 3.7(3.7), $\overline{\sigma} \in \mathcal{F}(X)$. By Def. 4.1 we conclude that $e \in \mathcal{R}(X)$. $\qquad\square$

We now introduce the notion of *trace with past*, respect to a set of already happened events C, and a credit X.

Definition B.1. (Trace with past)
For all $C \subseteq_{fin} E$, $X \subseteq E$, we say that $\sigma = \langle e_0 \ldots e_n \rangle \in E^*$ is an X-*trace with past* C iff $CF(C \cup \overline{\sigma})$, $C \cap \overline{\sigma} = \emptyset$, $DF(\sigma)$, and

$$\forall i \leq n. \ (e_i \in X \ \lor \ C \cup \overline{\sigma_i} \vdash e_i \ \lor \ C \cup \overline{\sigma} \Vdash e_i) \tag{9}$$

We denote with $\mathcal{T}^C_{\mathcal{E}}(X)$ the set of X-traces with past C. Note that, when $X \subseteq C$, we have $\mathcal{T}^C(X) = \mathcal{T}^C$.

Definition B.2. (Configuration with past)
For all $P \subseteq_{fin}$ and $X \subseteq E$, we define the set $\mathcal{F}^P_{\mathcal{E}}(X)$ of X-configurations with past P as follows:

$$\mathcal{F}^P_{\mathcal{E}}(X) \ = \ \{C \subseteq E \setminus P \mid CF(C) \land \forall e \in C. \ \exists \sigma \in \mathcal{T}^P_{\mathcal{E}}(X). \ e \in \overline{\sigma} \subseteq C\}$$

Lemma B.3. Let $X, C \subseteq E$. Then, $\mathcal{T}^C(X) = \mathcal{T}^C(X \setminus C)$

Proof:
Straightforward from Def. B.1. □

Lemma B.4. For all $X, C \subseteq E$, and $\sigma, \eta \in E^*$:

$$\eta \in \mathcal{T}(X) \ \land \ \sigma \in \mathcal{T}^C \ \land \ \overline{\eta} = C \implies \eta\sigma \in \mathcal{T}(X)$$

Proof:
Let $\sigma = \langle e_0 \ldots e_n \rangle \in \mathcal{T}^C$. By Def. B.1 we have $CF(C \cup \overline{\sigma})$, $C \cap \overline{\sigma} = \emptyset$, $DF(\sigma)$, and

$$\forall i \leq n. \ (C \cup \overline{\sigma_i} \vdash e_i \ \lor \ C \cup \overline{\sigma} \Vdash e_i) \tag{10}$$

Let $\eta = \langle a_0 \ldots a_k \rangle \in \mathcal{T}(X)$ be such that $\overline{\eta} = C$. We have to prove that $\nu = \eta\sigma \in \mathcal{T}(X)$, i.e. $CF(\overline{\nu})$, $DF(\nu)$ and

$$\forall i \leq k. \ (a_i \in X \ \lor \ \overline{\nu_i} \vdash a_i \ \lor \ \overline{\nu} \Vdash a_i) \ \land \tag{11}$$
$$\forall k < i \leq n. \ (e_i \in X \ \lor \ \overline{\nu_i} \vdash e_i \ \lor \ \overline{\nu} \Vdash e_i) \tag{12}$$

Since $CF(C \cup \overline{\eta})$ then $CF(\overline{\nu})$. Since $C \cup \overline{\sigma}$ and $DF(\sigma)$, we have $DF(\nu)$. Since $\eta \in \mathcal{T}(X)$, (11) trivially holds. For (12), we have two further subcases, based on how the event e_i was justified in (10):

- $C \cup \overline{\sigma_i} \vdash e_i$. Since $i > k$, we have $C \cup \overline{\sigma_i} = \overline{\nu_i}$, and then $\overline{\nu_i} \vdash e_i$.

- $C \cup \overline{\sigma} \Vdash e_i$. Since $C \cup \overline{\sigma} = \overline{\nu}$, we have $\overline{\nu} \Vdash e_i$.

□

Lemma B.5. Let (C, X) be a reachable state of $\mathrm{LTS}_{\mathcal{E}}$. Then:

$$\sigma \in \mathcal{T}^C \iff \exists X_0 \subseteq X. \ (C, X) \xrightarrow{\sigma} (C \cup \overline{\sigma}, X_0)$$

Proof:

($\Rightarrow$) Let $\sigma \in \mathcal{T}^C$. Since (C, X) is reachable, there exists η such that $(\emptyset, \emptyset) \xrightarrow{\eta} (C, X)$ and $\overline{\eta} = C$; so by Lemma 5.6, $\eta \in \mathcal{T}(X)$. By Lemma B.4, $\eta\sigma \in \mathcal{T}(X)$. Let $X_0 \subseteq X$ be the least credit of $\eta\sigma$. By Lemma 5.6 we have $(\emptyset, \emptyset) \xrightarrow{\eta\sigma} (\overline{\eta\sigma}, X_0)$. Since $\mathrm{LTS}_{\mathcal{E}}$ is deterministic, we conclude that $(C, X) \xrightarrow{\sigma} (C \cup \overline{\sigma}, X_0)$. The thesis follows because $\overline{\eta\sigma} = C \cup \overline{\sigma}$.

($\Leftarrow$) Since (C, X) is reachable, by Lemma 5.6 there exists $\eta \in \mathcal{T}(X)$ such that $\overline{\eta} = C$ and $(\emptyset, \emptyset) \xrightarrow{\eta} (C, X)$. By hypothesis there exists X_0 such that $(C, X) \xrightarrow{\sigma} (C \cup \overline{\sigma}, X_0)$. Summing up, $(\emptyset, \emptyset) \xrightarrow{\eta\sigma} (C \cup \overline{\sigma}, X_0)$. By Lemma 5.6, X_0 is the least credit for $\eta\sigma$. By Lemma 3.2(b), since $\eta\sigma \in \mathcal{T}(X_0)$ and $X_0 \subseteq X$, we have $\eta\sigma \in \mathcal{T}(X)$. By Def. B.1, we conclude that $\sigma \in \mathcal{T}^C(X)$, and the thesis follows from Lemma B.3 because $X \subseteq C$. $\qquad\square$

Definition B.6. For all $C \subseteq_{fin} E$ and $X \subseteq E$, we define:

$$\mathcal{R}_{\mathcal{E}}^C(X) = \bigcup \mathcal{F}_{\mathcal{E}}^C(X)$$

The following lemma relates reachability with past to (plain) reachability. Note that the inclusion $\mathcal{R}(X) \supseteq \mathcal{R}^C(X) \cup C$ does not hold. For instance, in the event structure with enabling $\{a\} \vdash b$ and with $C = \{a\}$, we have that $\mathcal{R}(\emptyset) = \emptyset$, but $\mathcal{R}^C(\emptyset) = \{b\}$.

Lemma B.7. For all $C \subseteq_{fin} E$ and $X \subseteq E$, $\mathcal{R}^C(X) \cup C = \mathcal{R}(C \cup X)$.

Proof:

For ($\supseteq$), let $e \in \mathcal{R}(C \cup X)$. Then, there exists $\eta \in \mathcal{T}(C \cup X)$ such that $e \in \overline{\eta}$. If $e \in C$, we already have the thesis. Otherwise, assume $e \notin C$. Let η' be the sequence obtained by removing from η all the events in C, while preserving the order of the other events. It is easy to show that $\eta' \in \mathcal{T}^C(X)$ and $e \in \overline{\eta'}$. Therefore, $e \in \mathcal{R}^C(X)$.

For ($\subseteq$), let $e \in \mathcal{R}^C(X) \cup C$. If $e \in C$, the thesis holds trivially. Otherwise, there exists $\sigma \in \mathcal{T}^C(X)$ such that $e \in \overline{\sigma}$ and $\overline{\sigma} \cap C = \emptyset$. Let $\sigma' = \sigma_C \, \sigma$, where σ_C is an arbitrary sequentialisation of the events in C. It is easy to show that $\sigma' \in \mathcal{T}(C \cup X)$. Then, $e \in \mathcal{R}(C \cup X)$. $\qquad\square$

The following lemma provides an alternative characterisation of urgent events, in terms of traces with past. An event e is urgent in (C, X) iff there exists a trace with past C such that the first element of the trace is e, and the credit X is honoured by the events in the trace together with those in C.

Lemma B.8. For all $e \in E$, and for all reachable state (C, X) of $\mathrm{LTS}_{\mathcal{E}}$,

$$e \in \mathcal{U}_{\mathcal{E}}^C(X) \iff \exists \sigma. \ e\sigma \in \mathcal{T}^C \ \wedge \ C \cup \overline{e\sigma} \Vdash X$$

Proof:

Straightforward after Lemma B.5 and Lemma 5.6(a). $\qquad\square$

Lemma B.9. For all C, X, σ, $(C, X) \xrightarrow{\sigma}_{\mathcal{U}_{\mathcal{E}}} (C', \emptyset) \iff (C, X) \xrightarrow{\sigma}_{\mathcal{E}} (C', \emptyset)$.

Proof:

The direction ($\Rightarrow$) of (B.9) follows because $\rightarrow_{\mathcal{U}_{\mathcal{E}}} \subseteq \rightarrow_{\mathcal{E}}$. The other direction can be easily proved by induction on the length of σ. $\qquad\square$

Proof of Lemma 5.13:
To prove ($\Rightarrow$), we distinguish between two cases. If $\sigma = \varepsilon$, the statement holds trivially. Otherwise, assume $\sigma = \nu e$, and let X be the least credit for $\nu \in \mathcal{T}(X)$. Since $\nu e \in \mathcal{T}_\varepsilon$, by Lemma 5.6 it must be $(\emptyset, \emptyset) \xrightarrow{\nu}_\varepsilon (\overline{\nu}, X) \xrightarrow{e}_\varepsilon (\overline{\nu e}, \emptyset)$. By Lemma B.5, we have that $e \in \mathcal{T}^{\overline{\nu}}$, and clearly $\overline{\nu e} \Vdash X$. Therefore, by Lemma B.8 we conclude that $e \in \mathcal{U}^{\overline{\nu}}(X)$. By Lemma B.9, we obtain the thesis $(\emptyset, \emptyset) \xrightarrow{\nu}_{\mathcal{U}_\varepsilon} \xrightarrow{e}_{\mathcal{U}_\varepsilon}$.

The direction ($\Leftarrow$) follows from Lemma B.5, since $\rightarrowtail_{\mathcal{U}_\varepsilon} \subseteq \rightarrow_\varepsilon$. $\qquad\square$

Proof of Lemma 5.14:
Assume that $(\emptyset, \emptyset) \xrightarrow{\sigma}_{\mathcal{U}_\varepsilon} (\overline{\sigma}, X)$, for some X. If $X = \emptyset$, we conclude by choosing $\eta = \varepsilon$. Otherwise, let $\sigma = \langle e_0 \cdots e_n \rangle$, and let $C_i = \overline{\sigma_i}$. Then, $(\emptyset, \emptyset) \xrightarrow{e_0}_{\mathcal{U}} (C_1, X_1) \xrightarrow{e_1}_{\mathcal{U}} (C_2, X_2) \xrightarrow{e_2}_{\mathcal{U}} \cdots \xrightarrow{e_n}_{\mathcal{U}} (\overline{\sigma}, X)$. By Def. 5.10, we have that for all $i \leq n$, $e_i \in \mathcal{U}^{C_i}(X_i)$. In particular, for $i = n$ we have that there exists η such that $(\overline{\sigma}, X) \xrightarrow{\eta} (\overline{\sigma\eta}, \emptyset)$. The thesis follows directly by Lemma B.9. $\qquad\square$

Proof of Lemma 5.15:
For $\subseteq$ of item (5.15), by Lemma 5.13 it follows that for all σ, η, if $\sigma\eta \in \mathcal{T}_\varepsilon$, then $(\emptyset, \emptyset) \xrightarrow{\sigma}_{\mathcal{U}_\varepsilon}$. It is easy to check that this implies the thesis.

For $\supseteq$, assume that $(\emptyset, \emptyset) \xrightarrow{\sigma}_{\mathcal{U}} (\overline{\sigma}, X)$. By Lemma 5.14, there exists η such that $(\overline{\sigma}, X) \xrightarrow{\eta}_{\mathcal{U}} (\overline{\sigma\eta}, \emptyset)$. By Lemma 5.13, $\sigma\eta \in \mathcal{T}_\varepsilon$. Therefore, all the events in $\overline{\sigma}$ are comprised in $\mathcal{R}_\varepsilon$. $\qquad\square$

Lemma B.10. $\sigma \in \mathcal{T}^C(X) \wedge \sigma' \in \mathcal{T}^C(X) \wedge CF(\overline{\sigma\sigma'}) \implies (\sigma\sigma')\!\downarrow \in \mathcal{T}^C(X)$.

Proof:
Direct consequence of Def. B.1 and of Lemma 3.2. $\qquad\square$

The following lemma simplifies the characterisation of urgent events in terms of traces given by Lemma B.8. This simplified characterisation only holds for conflict-free CES, and for those states (C, X) which are reachable in the LTS $\rightarrowtail_{\mathcal{U}_\varepsilon}$. Under this hypothesis, it is no longer needed to check that the credits in X are honoured: this is already guaranteed by the fact that there exists a trace $e\sigma$ in $\mathcal{T}^C$. Therefore, for conflict-free CES the LTS $\rightarrowtail_{\mathcal{U}_\varepsilon}$ can be simplified by eliminating the component X from the states. Note that, if (C, X) is *not* reachable in $\rightarrowtail_{\mathcal{U}_\varepsilon}$, then the ($\Leftarrow$) direction of Lemma B.11 may be false. For instance, in the CES with enablings $a \vdash b$ and $b \Vdash a$, consider the state $(\{b\}, \{b\})$, which is not reachable in $\rightarrowtail_{\mathcal{U}_\varepsilon}$. Then, $\langle a \rangle \in \mathcal{T}^{\{b\}}$, but a is *not* urgent in $(\{b\}, \{b\})$.

Lemma B.11. For a a conflict-free CES $\mathcal{E}$, and a reachable state (C, X) of $\rightarrowtail_{\mathcal{U}_\varepsilon}$:

$$e \in \mathcal{U}^C_\mathcal{E}(X) \iff \exists \sigma. \, e\sigma \in \mathcal{T}^C_\mathcal{E}$$

Proof:
The ($\Rightarrow$) direction is straightforward after Lemma B.8. For ($\Leftarrow$), let σ be such that $(\emptyset, \emptyset) \xrightarrow{\sigma}_{\mathcal{U}} (C, X)$ and $\overline{\sigma} = C$, and assume that $e\nu \in \mathcal{T}^C$, for some ν. By Lemma 5.14, there exists η such that $(C, X) \xrightarrow{\eta}_{\mathcal{U}} (\overline{\sigma\eta}, \emptyset)$. By Lemma B.5, $\eta \in \mathcal{T}^C$, and by Lemma 5.6(a), $C \cup \overline{\eta} \Vdash X$. By Lemma B.10, since $CF(e\nu\eta)$ then $e\nu\eta\!\downarrow \in \mathcal{T}^C$. By Lemma 5.6(b), $\sigma \in \mathcal{T}(X)$. Therefore, Lemma B.4 gives that $\sigma(e\nu\eta)\!\downarrow \in \mathcal{T}(X)$, from which Lemma 3.5 yields $\sigma(e\nu\eta)\!\downarrow \in \mathcal{T}$. Finally, Lemma 5.13 gives that $(C, X) \xrightarrow{(e\nu\eta)\!\downarrow}_{\mathcal{U}}$, which concludes. $\qquad\square$

Proof of Lemma 5.17:

For the inclusion ($\subseteq$), let $e \in \hat{\mathcal{U}}^C(X)$. If $e \in C$, we already have the thesis. Otherwise, since (C, X) is a reachable state of $\twoheadrightarrow_{\mathcal{U}_{\mathcal{E}}}$, by Lemma B.11 it suffices to show some σ such that $e\sigma \in \mathcal{T}^C$. We now proceed by cases on the rule used to deduce $e \in \hat{\mathcal{U}}^C_{\mathcal{E}}(X)$.

- $(\vdash_{\hat{u}})$. Let $\sigma = \varepsilon$. Then, $e\sigma \in \mathcal{T}^C$ holds, because $C \vdash e$.

- $(\Vdash_{\hat{u}})$. Since $\mathcal{R}(C \cup X) \Vdash e$, by Notation 2.3 there exists $D \subseteq_{fin} \mathcal{R}(C \cup X)$ such that $D \Vdash e$. By Lemma B.7, $\mathcal{R}(C \cup X) = \mathcal{R}^C(X) \cup C$. By Def. B.6, $\mathcal{R}^C(X) = \bigcup \mathcal{F}^C(X)$. Since configurations with past enjoy coherence and $\mathcal{E}$ is conflict-free, then $D \setminus C \subseteq_{fin} \mathcal{R}^C(X) \in \mathcal{F}^C(X)$. Thus, by Def. B.2, there exists $\sigma \in \mathcal{T}^C(X)$ such that $\overline{\sigma} \supseteq D \setminus C$. Since $X \subseteq C$, this implies that $\sigma \in \mathcal{T}^C$. Since $C \cup \overline{e\sigma} \supseteq C \cup D \Vdash e$, then we conclude that there exists σ' such that $e\sigma' = (e\sigma){\downarrow} \in \mathcal{T}^C$.

For the inclusion ($\supseteq$), let $e \in \mathcal{U}^C(X) \cup C$. If $e \in C$, the thesis follows by rule ($\in_{\hat{u}}$). Otherwise, if $e \in \mathcal{U}^C(X)$, by Lemma B.11, there exists σ such that $e\sigma \in \mathcal{T}^C$. There are the following two cases, according to how e was justified in $e\sigma$.

- $C \vdash e$. By rule ($\vdash_{\hat{u}}$), we conclude that $e \in \hat{\mathcal{U}}^C(X)$, for all X.

- $C \cup \overline{e\sigma} \Vdash e$. Since $e\sigma \in \mathcal{T}^C$, then $\overline{e\sigma} \in \mathcal{F}^C$, and so by Def. B.6, $\overline{e\sigma} \subseteq \mathcal{R}^C$. By Lemma B.7, $\mathcal{R}(C) = \mathcal{R}^C \cup C \supseteq \overline{e\sigma} \cup C \Vdash e$. Thus, by rule ($\Vdash_{\hat{u}}$), we conclude that $e \in \hat{\mathcal{U}}^C(\emptyset)$. $\square$

C. Proofs for Section 6

C.1. Propositional Contract Logic

Definition C.1. The Gentzen-style sequent calculus of PCL is defined by the rules in Fig. 5

As proved in [7], the sequent calculus of PCL enjoys cut elimination. A cut on a formula p is replaced by cuts on strict subformulae of p, and cuts on p having a shorter proof tree. This makes PCL decidable.

Theorem C.2. (Cut Elimination [7])
If p is provable in PCL, then there exists a proof of p not using the (CUT) rule.

Hereafter, φ will range over conjunctions of atoms, and Φ will range over sets of conjunctions of atoms. With a little abuse of notation, we shall use sets of events X in PCL formulae, actually standing for the formula $\bigwedge X$.

Proof of Lemma 6.3:

Under the hypothesis of the lemma, by Theorem 4.7 we have $\mathcal{R}_{\mathcal{E}}(\overline{\Phi}) = \hat{\mathcal{R}}_{\mathcal{E}}(\overline{\Phi})$. Consequently, we will actually prove that $\overline{\varphi} \subseteq \hat{\mathcal{R}}_{\mathcal{E}}(\overline{\Phi})$ iff $[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash_{\text{PCL}} \varphi$.

For the ($\Leftarrow$) direction, assume that $[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash_{\text{PCL}} \varphi$.

By Theorem C.2, consider a proof tree Δ of $[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash_{\text{PCL}} \varphi$ without occurrences of the (CUT) rule. The RHS of each sequent in Δ has the form $\bigwedge_{i \in I} e_i$, and so Δ only contains occurrences of the rules (ID), ($\wedge$L1), ($\wedge$L2), ($\rightarrow$L), (FIX). We prove $\overline{\varphi} \subseteq \mathcal{R}_{\mathcal{E}}(\overline{\Phi}) \iff [\mathcal{E}]_{\mathcal{R}}, \Phi \vdash_{\text{PCL}} \varphi$ by induction on the depth of Δ.

$$\frac{}{\Gamma, p \vdash p} \text{ (ID)} \qquad \frac{\Gamma \vdash p \quad \Gamma, p \vdash q}{\Gamma \vdash q} \text{ (CUT)}$$

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

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

$$\frac{\Gamma, p \rightarrow q \vdash p \quad \Gamma, p \rightarrow q, q \vdash r}{\Gamma, p \rightarrow q \vdash r} \text{ (}\rightarrow\text{L)} \qquad \frac{\Gamma, p \vdash q}{\Gamma \vdash p \rightarrow q} \text{ (}\rightarrow\text{R)}$$

$$\frac{\Gamma, \neg p \vdash p}{\Gamma, \neg p \vdash r} \text{ (}\neg\text{L)} \qquad \frac{\Gamma, p \vdash \bot}{\Gamma \vdash \neg p} \text{ (}\neg\text{R)} \qquad \frac{}{\Gamma, \bot \vdash p} \text{ (}\bot\text{L)} \qquad \frac{}{\Gamma \vdash \top} \text{ (}\top\text{R)} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash p} \text{ (WEAKR)}$$

$$\frac{\Gamma \vdash q}{\Gamma \vdash p \twoheadrightarrow q} \text{ (ZERO)} \qquad \frac{\Gamma, p \twoheadrightarrow q, a \vdash p \quad \Gamma, p \twoheadrightarrow q, q \vdash b}{\Gamma, p \twoheadrightarrow q \vdash a \twoheadrightarrow b} \text{ (PREPOST)}$$

$$\frac{\Gamma, p \twoheadrightarrow q, r \vdash p \quad \Gamma, p \twoheadrightarrow q, q \vdash r}{\Gamma, p \twoheadrightarrow q \vdash r} \text{ (FIX)}$$

Figure 5. Genzten-style proof system for PCL.

The base case concerns the axiom (ID), which gives:

$$\frac{\varphi \in \Phi}{[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash \varphi} \text{ (ID)}$$

Since $\varphi \in \Phi$, then $\overline{\varphi} \subseteq \overline{\Phi}$, so by Lemmata A.2(a) and A.2(b) we have $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\varphi}) \subseteq \hat{\mathcal{R}}(\overline{\Phi})$.

For the inductive case, we proceed by cases on the last rule used in Δ. There are the following exhaustive cases:

- case ($\wedge$L1). We have that $\Phi = \Phi', q \wedge r$ for some Φ', so:

$$\frac{[\mathcal{E}]_{\mathcal{R}}, \Phi', q \wedge r, q \vdash \varphi}{[\mathcal{E}]_{\mathcal{R}}, \Phi', q \wedge r \vdash \varphi} \text{ (}\wedge\text{L1)}$$

By the induction hypothesis, $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \overline{q}) = \hat{\mathcal{R}}(\overline{\Phi})$.

- case ($\wedge$L2) similar to the previous one.

- case ($\rightarrow$L). We have $q \rightarrow a \in [\mathcal{E}]_{\mathcal{R}}$ for some conjunction of atoms q and atom a, and

$$\frac{[\mathcal{E}]_{\mathcal{R}}, \Phi, q \rightarrow a \vdash q \quad [\mathcal{E}]_{\mathcal{R}}, \Phi, a \vdash \varphi}{[\mathcal{E}]_{\mathcal{R}}, \Phi, q \rightarrow a \vdash \varphi} \text{ (}\rightarrow\text{L)}$$

By applying the induction hypothesis twice, we have $\overline{q} \subseteq \hat{\mathcal{R}}(\overline{\Phi})$, and $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \{a\})$.

Since $q \to a \in [\mathcal{E}]_{\mathcal{R}}$, by Def 6.2 it must be the case that $\overline{q} \vdash a \in \mathcal{E}$. By saturation, $\hat{\mathcal{R}}(\overline{\Phi}) \vdash a$. Thus by $(\vdash_{\hat{\mathcal{R}}})$:

$$\frac{\hat{\mathcal{R}}(\overline{\Phi}) \vdash a}{a \in \hat{\mathcal{R}}(\overline{\Phi})} \; (\vdash_{\hat{\mathcal{R}}})$$

By Lemma A.3, $\hat{\mathcal{R}}(\overline{\Phi} \cup \{a\}) = \hat{\mathcal{R}}(\overline{\Phi})$, from which we conclude $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\Phi})$.

- case (FIX). We have $q \twoheadrightarrow a \in [\mathcal{E}]_{\mathcal{R}}$ for some conjunction of atoms q and atom a, and

$$\frac{[\mathcal{E}]_{\mathcal{R}}, \; \Phi, \; q \twoheadrightarrow a, \; \varphi \vdash q \quad [\mathcal{E}]_{\mathcal{R}}, \; \Phi, \; a \vdash \varphi}{[\mathcal{E}]_{\mathcal{R}}, \; \Phi, \; q \twoheadrightarrow a \vdash \varphi} \; (\text{FIX})$$

By applying the induction hypothesis twice, $\overline{q} \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \overline{\varphi})$, and $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \{a\})$.

From the last inclusion, Lemma A.3 yields $\hat{\mathcal{R}}(\overline{\Phi} \cup \{a\} \cup \overline{\varphi}) = \hat{\mathcal{R}}(\overline{\Phi} \cup \{a\})$. Since $\overline{q} \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \overline{\varphi}) \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \{a\} \cup \overline{\varphi})$, then we also have $\overline{q} \subseteq \hat{\mathcal{R}}(\overline{\Phi} \cup \{a\})$.

Since $q \twoheadrightarrow a \in [\mathcal{E}]_{\mathcal{R}}$, by Def 6.2, it must be the case that $\overline{q} \Vdash a \in \mathcal{E}$. Thus, by saturation $\hat{\mathcal{R}}(\overline{\Phi} \cup \{a\}) \Vdash a$. By rule $(\Vdash_{\hat{\mathcal{R}}})$, we have:

$$\frac{\hat{\mathcal{R}}(\overline{\Phi} \cup \{a\}) \Vdash a}{a \in \hat{\mathcal{R}}(\overline{\Phi})} \; (\Vdash_{\hat{\mathcal{R}}})$$

By Lemma A.3, $\hat{\mathcal{R}}(\overline{\Phi} \cup \{a\}) = \hat{\mathcal{R}}(\overline{\Phi})$, therefore $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\Phi})$.

For the $(\Rightarrow)$ direction, let $\overline{\varphi} \subseteq \hat{\mathcal{R}}(\overline{\Phi})$, and let $e \in \overline{\varphi}$. We will prove that $[\mathcal{E}]_{\mathcal{R}}, \; \Phi \vdash_{\text{PCL}} e$, which implies the thesis. We proceed by induction on the depth of the derivation of $e \in \hat{\mathcal{R}}(\overline{\Phi})$. According to the last rule used, we have the following cases:

- case $(\in_{\hat{\mathcal{R}}})$. The premise of rule $(\in_{\hat{\mathcal{R}}})$ prescribes that $e \in \overline{\Phi}$. By suitable application of rules (ID), ($\wedge$L1) and ($\wedge$L2) we obtain the thesis $[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash e$.

- case $(\vdash_{\hat{\mathcal{R}}})$. We have:

$$\frac{\hat{\mathcal{R}}(\overline{\Phi}) \vdash e}{e \in \mathcal{R}(\overline{\Phi})} \; (\vdash_{\hat{\mathcal{R}}})$$

Since $\hat{\mathcal{R}}(\overline{\Phi}) \vdash e$, there must exists a minimal $D \subseteq_{fin} \hat{\mathcal{R}}(\overline{\Phi})$ such that $D \vdash e \in \mathcal{E}$. By Def. 6.2, we have that $(\bigwedge D) \to e \in [\mathcal{E}]_{\mathcal{R}}$. By the induction hypothesis we have that for all $d \in D$, $[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash d$. Then:

$$\frac{\dfrac{I.H.}{[\mathcal{E}]_{\mathcal{R}}, \; \Phi \vdash \bigwedge D} \quad \dfrac{}{[\mathcal{E}]_{\mathcal{R}}, \Phi, \; e \vdash e} \; (\text{ID})}{[\mathcal{E}]_{\mathcal{R}}, \; \Phi \vdash e} \; (\to\text{L})$$

- case $(\Vdash_{\hat{\mathcal{R}}})$. We have:

$$\frac{\hat{\mathcal{R}}(\overline{\Phi} \cup \{e\}) \Vdash e}{e \in \hat{\mathcal{R}}(\overline{\Phi})} \; (\Vdash_{\hat{\mathcal{R}}})$$

Since $\hat{\mathcal{R}}(\overline{\Phi} \cup \{e\}) \Vdash e$, there must exist a minimal $D \subseteq_{fin} \hat{\mathcal{R}}(\overline{\Phi} \cup \{e\})$ such that $D \Vdash e \in \mathcal{E}$. Then, by Def. 6.2, we have that $(\bigwedge D) \twoheadrightarrow e \in [\mathcal{E}]_{\mathcal{R}}$. By the induction hypothesis we have that, for all $d \in D$, $[\mathcal{E}]_{\mathcal{R}}, \Phi, e \vdash d$. Then:

$$\frac{\dfrac{I.H.}{[\mathcal{E}]_{\mathcal{R}}, \Phi, e \vdash \bigwedge D} \qquad \dfrac{}{[\mathcal{E}]_{\mathcal{R}}, \Phi, e \vdash e}\ (\text{ID})}{[\mathcal{E}]_{\mathcal{R}}, \Phi \vdash e}\ (\text{FIX})$$

$\square$

Proof of Lemma 6.6:

Item (a) follows by a straightforward inductive argument on the depth of the proof of $[\mathcal{E}]_{\mathcal{F}}, \Phi \vdash_{\text{PCL}} \varphi$.

For item (b), by Theorem C.2 consider a proof tree Δ of $[\mathcal{E}]_{\mathcal{F}}, \Phi \vdash_{\text{PCL}} \varphi$ without occurrences of the (CUT) rule. The RHS of each sequent in Δ is a conjunction of atoms, and so Δ only contains occurrences of the rules (ID), ($\wedge$L1), ($\wedge$L2), ($\wedge$R), ($\rightarrow$L), (FIX). We proceed by induction on the depth of Δ; there are the following exhaustive cases:

- (ID). The base case concerns the axiom (ID), which gives $[\mathcal{E}]_{\mathcal{F}}, \Phi \vdash_{\text{PCL}} \varphi$ provided that $\varphi \in \Phi$. We have that $\overline{\varphi}^{\flat} \subseteq \overline{\Phi}^{\flat} \subseteq \overline{\Phi}^{!}$.

- ($\wedge$L1), ($\wedge$L2), and ($\wedge$R). Straightforward by the induction hypothesis.

- ($\rightarrow$L). We have $p \rightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ for some conjunction of atoms p and atom e, and:

$$\frac{[\mathcal{E}]_{\mathcal{F}}, \Phi, p \rightarrow e \vdash p \qquad [\mathcal{E}]_{\mathcal{F}}, \Phi, e \vdash \varphi}{[\mathcal{E}]_{\mathcal{F}}, \Phi \vdash \varphi}\ (\rightarrow\text{L})$$

  By applying item (a) on the leftmost premise of rule ($\rightarrow$L) it follows that $\overline{p}^{!} \subseteq \overline{\Phi}^{!}$. The formula $p \rightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ must have been obtained as the encoding of an enabling $Z \vdash e$ in $\mathcal{E}$. Thus, by Def. 6.5 it must be the case that $p = {!}e \wedge Z \wedge {!}Z$. We then have $e \in \overline{p}^{!} \subseteq \overline{\Phi}^{!}$, and so since by hypothesis $\overline{\Phi}^{\flat} \subseteq \overline{\Phi}^{!}$:

$$(\overline{\Phi} \cup \{e\})^{\flat} = \overline{\Phi}^{\flat} \cup \{e\} \subseteq \overline{\Phi}^{!} \cup \{e\} = \overline{\Phi}^{!}$$

  We can then apply the induction hypothesis on the rightmost premise of rule ($\rightarrow$L), and obtain the thesis $\overline{\varphi}^{\flat} \subseteq (\overline{\Phi} \cup \{e\})^{!} = \overline{\Phi}^{!}$.

- (FIX). We have that $p \twoheadrightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ for some conjunction of atoms p and atom e, and:

$$\frac{[\mathcal{E}]_{\mathcal{F}}, \Phi, p \twoheadrightarrow e, \varphi \vdash p \qquad [\mathcal{E}]_{\mathcal{F}}, \Phi, e \vdash \varphi}{[\mathcal{E}]_{\mathcal{F}}, \Phi \vdash \varphi}\ (\text{FIX})$$

  By applying item (a) to the leftmost premise of (FIX), we obtain $\overline{p}^{!} \subseteq \overline{\Phi}^{!} \cup \overline{\varphi}^{!}$. The formula $p \twoheadrightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ must have been obtained as the encoding of an enabling $Z \Vdash e$ in $\mathcal{E}$. Thus, by Def. 6.5 it must be the case that $p = {!}e \wedge Z \wedge {!}Z$. We then have $e \in \overline{p}^{!} \subseteq \overline{\Phi}^{!} \cup \overline{\varphi}^{!}$. By applying item (a) to the rightmost premise of (FIX), we obtain $\overline{\varphi}^{!} \subseteq \overline{\Phi}^{!} \cup \{e\}^{!} = \overline{\Phi}^{!}$. Summing up,

$$(\overline{\Phi} \cup \{e\})^{\flat} = \overline{\Phi}^{\flat} \cup \{e\} \subseteq \overline{\Phi}^{!} \cup \{e\} \subseteq \overline{\Phi}^{!} \cup \overline{p}^{!} \subseteq \overline{\Phi}^{!} \cup \overline{\varphi}^{!} \subseteq \overline{\Phi}^{!}$$

  We can then apply the induction hypothesis on the rightmost premise of rule (FIX), and obtain the thesis $\overline{\varphi}^{\flat} \subseteq (\overline{\Phi} \cup \{e\})^{!} = \overline{\Phi}^{!}$.

$\square$

Proof of Theorem 6.7:

For the ($\Leftarrow$) direction, we shall first prove the following statement. For all sets of conjunctions of atoms Φ, and for all conjunctions of atoms φ:

$$[\mathcal{E}]_{\mathcal{F}},\ \Phi \vdash_{\text{PCL}} \varphi\ \wedge\ \overline{\Phi}^{\flat} \subseteq \overline{\Phi}^{!}\ \wedge\ CF(\overline{\Phi}^{!}) \implies \exists C' \in \mathcal{F}(\overline{\Phi}^{\flat}).\ \overline{\varphi}^{\flat} \subseteq C' \subseteq \overline{\Phi}^{!} \tag{13}$$

By Theorem C.2, consider a proof tree Δ of $[\mathcal{E}]_{\mathcal{F}},\ \Phi \vdash_{\text{PCL}} \varphi$ without occurrences of the (CUT) rule. The RHS of each sequent in Δ is a conjunction of atoms, and so Δ only contains occurrences of the rules (ID), ($\wedge$L1), ($\wedge$L2), ($\wedge$R), ($\rightarrow$L), (FIX). We prove (13) by induction on the depth of Δ.

The base case concerns the axiom (ID), which gives $[\mathcal{E}]_{\mathcal{F}},\ \Phi \vdash_{\text{PCL}} \varphi$ whenever $\varphi \in \Phi$. Let $C' = \overline{\varphi}^{\flat}$. Then we have $C' = \overline{\varphi}^{\flat} \subseteq \overline{\Phi}^{\flat} \subseteq \overline{\Phi}^{!}$. Since $CF(\overline{\Phi}^{!})$, then $CF(C')$. By Lemma 3.7(3.7) we have $C' \in \mathcal{F}(\overline{\varphi}^{\flat})$, and so Lemma 3.7(3.7) gives the thesis $C' \in \mathcal{F}(\overline{\Phi}^{\flat})$.

For the inductive case, we analyse the last rule used in Δ. 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 $\varphi = p \wedge q$:

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

By applying the induction hypothesis on the two premises, we obtain:

$$\exists C_1 \in \mathcal{F}(\overline{\Phi}^{\flat}).\ \overline{p}^{\flat} \subseteq C_1 \subseteq \overline{\Phi}^{!} \tag{14}$$

$$\exists C_2 \in \mathcal{F}(\overline{\Phi}^{\flat}).\ \overline{q}^{\flat} \subseteq C_2 \subseteq \overline{\Phi}^{!} \tag{15}$$

Let $C' = C_1 \cup C_2$. Since $C_1, C_2 \subseteq \overline{\Phi}^{!}$ and $CF(\overline{\Phi}^{!})$, we also have $CF(C')$. Then, by Theorem 3.12, $C' \in \mathcal{F}(\overline{\Phi}^{\flat})$. Furthermore, $\overline{\varphi}^{\flat} = \overline{p}^{\flat} \cup \overline{q}^{\flat} \subseteq C' \subseteq \overline{\Phi}^{!}$.

- ($\rightarrow$L). We have $p \rightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ for some conjunction of atoms p and atom e, and:

$$\frac{[\mathcal{E}]_{\mathcal{F}},\ \Phi,\ p \rightarrow e \vdash p \qquad [\mathcal{E}]_{\mathcal{F}},\ \Phi,\ e \vdash \varphi}{[\mathcal{E}]_{\mathcal{F}},\ \Phi \vdash \varphi}\ (\rightarrow\text{L})$$

The formula $p \rightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ must have been obtained as the encoding of an enabling $Z \vdash e$ in $\mathcal{E}$. Thus, by Def. 6.5 it must be the case that $p = {!}e \wedge Z \wedge {!}Z$. Since $[\mathcal{E}]_{\mathcal{F}},\ \Phi,\ p \rightarrow e \vdash p$, by Lemma 6.6 it follows that $\overline{p} \subseteq \overline{\Phi}$. Since $p = {!}e \wedge Z \wedge {!}Z$, we then have $e \in \overline{p}^{!} \subseteq \overline{\Phi}^{!}$, and so since by hypothesis $\overline{\Phi}^{\flat} \subseteq \overline{\Phi}^{!}$:

$$(\overline{\Phi} \cup \{e\})^{\flat} = \overline{\Phi}^{\flat} \cup \{e\} \subseteq \overline{\Phi}^{!} \cup \{e\} = \overline{\Phi}^{!}$$

Note also that $CF(\overline{\Phi}^{!})$ and $CF((\overline{\Phi} \cup \{e\})^{!})$. We can then apply the induction hypothesis twice on the two premises, and obtain:

$$\exists C_1 \in \mathcal{F}(\overline{\Phi}^{\flat}).\ \overline{p}^{\flat} \subseteq C_1 \subseteq \overline{\Phi}^{!} \tag{16}$$

$$\exists C_2 \in \mathcal{F}(\overline{\Phi}^{\flat} \cup \{e\}).\ \overline{\varphi}^{\flat} \subseteq C_2 \subseteq \overline{\Phi}^{!} \tag{17}$$

Let $C' = C_1 \cup C_2$. Since $C_1, C_2 \subseteq \overline{\Phi}^!$ and $CF(\overline{\Phi}^!)$, we also have $CF(C')$. Since $Z \vdash e$ and $Z = \overline{p}^\flat \subseteq C_1$, then by saturation we also have that $C_1 \vdash e$. Therefore, Lemma b gives $C' \in \mathcal{F}(\overline{\Phi}^\flat)$. The thesis follows by $\overline{\varphi}^\flat \subseteq \overline{\varphi}^\flat \cup \overline{p}^\flat \subseteq C' \subseteq \overline{\Phi}^!$.

- (FIX). We have that $p \twoheadrightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ for some conjunction of atoms p and atom e, and:

$$\frac{[\mathcal{E}]_{\mathcal{F}}, \, \Phi, \, p \twoheadrightarrow e, \, \varphi \vdash p \qquad [\mathcal{E}]_{\mathcal{F}}, \, \Phi, \, e \vdash \varphi}{[\mathcal{E}]_{\mathcal{F}}, \, \Phi \vdash \varphi} \text{ (FIX)}$$

The formula $p \twoheadrightarrow e \in [\mathcal{E}]_{\mathcal{F}}$ must have been obtained as the encoding of a circular enabling $Z \Vdash e$ in $\mathcal{E}$. Thus, by Def. 6.5 it must be the case that $p = \, !e \wedge Z \wedge !Z$. By applying Lemma 6.6 on the sequent $[\mathcal{E}]_{\mathcal{F}}, \, \Phi \vdash \varphi$ we have $\overline{\varphi} \subseteq \overline{\Phi}^!$. Therefore, $(\overline{\Phi} \cup \overline{\varphi})^\flat = \overline{\Phi}^\flat \cup \overline{\varphi}^\flat \subseteq \overline{\Phi}^! \cup \overline{\varphi} \subseteq \overline{\Phi}^!$, By applying Lemma 6.6 on the sequent $[\mathcal{E}]_{\mathcal{F}}, \, \Phi, \, \varphi \vdash p$, we have $\overline{p}^! \subseteq \overline{\Phi}^! \cup \overline{\varphi}^! \subseteq \overline{\Phi}^!$. Thus, $(\overline{\Phi} \cup \{e\})^\flat \subseteq \overline{\Phi}^! \cup \overline{p}^! \subseteq \overline{\Phi}^! \cup \overline{p} \subseteq \overline{\Phi}^!$.

Note also that, since $\overline{\varphi}^! \subseteq \overline{\Phi}^!$, then $CF(\overline{\Phi}^! \cup \overline{\varphi}^!)$ holds, as well as $CF(\overline{\Phi}^! \cup \{e\}^!)$. We can then apply the induction hypothesis twice on the two premises of rule (FIX):

$$\exists C_1 \in \mathcal{F}(\overline{\Phi}^\flat \cup \overline{\varphi}^\flat). \, \overline{p}^\flat \subseteq C_1 \subseteq \overline{\Phi}^! \tag{18}$$

$$\exists C_2 \in \mathcal{F}(\overline{\Phi}^\flat \cup \{e\}). \, \overline{\varphi}^\flat \subseteq C_2 \subseteq \overline{\Phi}^! \tag{19}$$

Let $C' = C_1 \cup C_2$. Since $C_1, C_2 \subseteq C$ and $CF(C)$, we also have $CF(C')$. Since $Z \Vdash e$ and $Z \subseteq \overline{p}^\flat \subseteq C_1$, by saturation we have $C_1 \Vdash e$. Since $\overline{\varphi}^\flat \subseteq C_2$, by (18) and by Lemma 3.7(3.7) we have $C_1 \in \mathcal{F}(\overline{\Phi}^\flat \cup C_2)$. Therefore, by Lemma c, we obtain $\overline{\varphi}^\flat \subseteq \overline{p}^\flat \cup \overline{\varphi}^\flat \subseteq C_1 \cup C_2 = C' \in \mathcal{F}(\overline{\Phi}^\flat)$.

We now prove that (13) implies the thesis. Assume that $[\mathcal{E}]_{\mathcal{F}}, !C, X \vdash_{\text{PCL}} C$, and $[\mathcal{E}]_{\mathcal{F}}, !C, X \nvdash_{\text{PCL}} \bot$. Let $Y = X \cap C$, let $\Phi = \, !C \cup \bigwedge Y$, and let $\varphi = \bigwedge C$. Then, $\overline{\Phi}^! = \overline{\varphi}^\flat = C$, and $\overline{\Phi}^\flat = Y$. By contradiction, assume that $\overline{\Phi}^!$ is not conflict-free. Since $\overline{\Phi}^! = C$, there must exist $a, b \in C$ such that $a \# b$, and so by Def. 6.5 we would have that $[\mathcal{E}]_{\mathcal{F}}, !C \vdash_{\text{PCL}} (!a \wedge !b) \to \bot$. This would imply that $[\mathcal{E}]_{\mathcal{F}}, !C \vdash_{\text{PCL}} \bot$, which would contradict the hypothesis of the lemma. Therefore, $CF(\overline{\Phi}^!)$. Also, $\overline{\Phi}^\flat = Y \subseteq C = \overline{\Phi}^\flat$. We can then apply (13), from which we find some $C' \in \mathcal{F}(X)$ such that $\overline{\varphi}^\flat \subseteq C' \subseteq \overline{\Phi}^!$. Since $C = \overline{\varphi}^\flat \subseteq C' \subseteq \overline{\Phi}^! = C$, we have $C \in \mathcal{F}(Y)$. Since $Y \subseteq X$, by Lemma 3.7(3.7) we obtain the thesis $C \in \mathcal{F}(X)$.

For the ($\Rightarrow$) direction, assume that $C \in \mathcal{F}_{\mathcal{E}}(X)$. Observe first that, since $CF(C)$, then for all choices of $X \subseteq E$ it cannot be the case that $[\mathcal{E}]_{\mathcal{F}}, !C, X \vdash_{\text{PCL}} \bot$. By Lemma 3.4, there exists $\sigma = \langle e_1 \ldots e_n \rangle \in \mathcal{T}(X)$ such that $\overline{\sigma} = C$. We proceed by induction on $|C \setminus X|$. For the base case $|C \setminus X| = 0$, since $C \subseteq X$, by rule (ID) we have that $[\mathcal{E}]_{\mathcal{F}}, !C, X \vdash_{\text{PCL}} C$. For the inductive case, we assume that

$$C \in \mathcal{F}(Y) \implies [\mathcal{E}]_{\mathcal{F}}, !C, Y \vdash_{\text{PCL}} C \tag{20}$$

holds for all Y such that $|C \setminus Y| < |C \setminus X|$. To do that, we prove the following statement, which implies (20):

$$\forall i \leq n. \, \Gamma \vdash_{\text{PCL}} e_i \tag{21}$$

To prove (21) we proceed by (strong) induction on i: assuming that (21) holds for $1..i-1$, we prove that it holds for i. We have the following three subcases, according to the way e_i has been justified in $\sigma \in \mathcal{T}(X)$.

- $e_i \in X$. The thesis follows trivially by (ID).

- $\overline{\sigma_i} \vdash e_i$ and $e_i \notin X$. By the induction hypothesis of (21), $\Gamma \vdash_{\text{PCL}} \overline{\sigma_i}$. By Def. 2.1, there must exist a minimal $Z \subseteq \overline{\sigma_i}$ such that $Z \vdash e_i$ is an enabling in $\mathcal{E}$. By Def. 6.5, $[\mathcal{E}]_{\mathcal{F}}$ contains the formula $p \rightarrow e_i$, with $p = {!e} \land Z \land {!Z}$. The sequent $\Gamma \vdash_{\text{PCL}} \overline{\sigma_i}$ can be weakened as $\Gamma \vdash_{\text{PCL}} Z$, because $Z \subseteq \overline{\sigma_i}$. Since $e \in C$, $Z \subseteq C$, and Γ contains $!C$, we also have that $\Gamma \vdash p$. Therefore, by rule ($\rightarrow$L) we obtain the thesis:

$$\frac{\Gamma, p \rightarrow e_i \vdash p \qquad \Gamma, p \rightarrow e_i, e_i \vdash e_i}{\Gamma, p \rightarrow e_i \vdash e_i}$$

- $C \Vdash e_i$ and $e_i \notin X$. By Def. 2.1, there must exist a minimal $Z \subseteq C$ such that $Z \Vdash e_i$ is a circular enabling in $\mathcal{E}$. By Def. 6.5, $[\mathcal{E}]_{\mathcal{F}}$ contains the formula $p \twoheadrightarrow e_i$, with $p = {!e_i} \land Z \land {!Z}$. Since $e_i \in C \setminus X$, we have that $|C \setminus X| > |C \setminus (X \cup \{e_i\})|$. Since $C \in \mathcal{F}(X)$, by Lemma 3.7(3.7) we also have that $C \in \mathcal{F}(X \cup \{e\})$. Thus, the induction hypothesis on the statement (20) gives $[\mathcal{E}]_{\mathcal{F}}, !C, X, e_i \vdash C$. This sequent can be weakened as $\Gamma, e_i \vdash Z$, because $Z \subseteq C$. Since $e \in C$, $Z \subseteq C$, and Γ contains $!C$, we also deduce that $\Gamma, e_i \vdash p$. Therefore, by rule (FIX) we obtain the thesis:

$$\frac{\Gamma, p \twoheadrightarrow e_i, e_i \vdash p \qquad \Gamma, p \twoheadrightarrow e_i, e_i \vdash e_i}{\Gamma, p \twoheadrightarrow e_i \vdash e_i}$$

$\square$