Circular causality in event structures

Massimo Bartoletti[1], Tiziana Cimoli[1], G. Michele Pinna[1], and Roberto Zunino[2]

[1] Dipartimento di Matematica e Informatica, Università degli Studi di Cagliari, Italy
[2] DISI, Università 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 show a correspondence between the configurations in our event structures, and the proofs of a fragment of Propositional Contract Logic.

1 Introduction

Circular reasoning often appears in the compositional modelling and verification of concurrent systems [1, 2, 6, 7]. Circularity is also a common situation when reasoning about contracts [4]. A task may depend on others which have already been executed (dependencies in the past), but also on behalf that some other tasks will be performed in the future. Circularity arises when two or more tasks mutually rely on the guarantees provided by each other (circular dependencies).

Event structures (ES) are one of the classical model for concurrency, since [8]. Notwithstanding the variety of ingredients appeared in the literature, ES are at least equipped with a relation (usually written $\vdash$) modelling *causality*, and another one modeling *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 assume/guarantee rules, by interpreting the enabling $b \vdash a$ as: "I will do a *after* you have done b".

However, circularity is usually prohibited in ES, either at the syntactic level, like in Winskel's prime event structures, or at the semantic level, like in Boudol's flow event structures [5]. Indeed, the classical notion of causality among events only captures dependencies in the past, but not of the other kind. For instance, in the ES with enablings $b \vdash a$ and $a \vdash b$, none of the events a and b is reachable, because of the circularity of the constraints.

We propose an extension of Winskel's event structures with a new *circular causality* relation ($\Vdash$). The ES prescribing $a \Vdash b$ (intuitively, "I will do a if you *promise* to do b") together with the other prescription $b \Vdash a$ has a configuration where both a and b have happened, despite of the circular dependencies. The configurations of these new ES do still enjoy the finiteness and finite-completeness properties of classical ES, thought they are not coincidence-free, which is correct from our point of view because of the presence of circular dependencies.

Our main technical result is an encoding of ES with circular causality into a fragment of Propositional Contract Logic PCL [4], through which we show that the problem of deciding if a set of events is a configuration can be reduced to provability in the logic (which is shown in [4] to be decidable).

2   Event structures with circular causality

In Def. 1 below we present our extension to Winskel's ES [8], to which we refer for the details about ES. We assume an irreflexive and symmetric conflict relation $\#$ on events, and for a set of events X, we define the predicate $CF(X)$ as follows: $CF(X) \triangleq (\forall e, e' \in X : \neg(e \# e'))$.

Definition 1. *An event structure with circular causality (*CES*) is a quadruple* $\mathcal{E} = (E, \#, \vdash, \Vdash)$ *where: (i)* E *is a set of events, (ii)* $\# \subseteq E \times E$ *is an irreflexive and symmetric relation, called* conflict *relation, (iii)* $\vdash \subseteq \wp_{fin}(E) \times E$ *is the* enabling *relation, (iv)* $\Vdash \subseteq \wp_{fin}(E) \times E$ *is the* circular enabling *relation. The relations* $\vdash$ *and* $\Vdash$ *are* saturated, *i.e. for all* $X, Y \subseteq_{fin} E$ *and for* $\circ \in \{\vdash, \Vdash\}$, $X \circ e \wedge X \subseteq Y \wedge CF(Y) \implies Y \circ e$.

A configuration C is a "snapshot" of the behaviour of the system modeled by an ES, where for each event $e \in C$ it is possible to find a finite justification, *i.e.* a sequence of events containing all the causes of e. We refine the notion in [8] to deal with circular causality. Intuitively, for all events e_i in the sequence $\langle e_0 \dots e_n \rangle$, either e_i is $\vdash$-enabled by its predecessors, or it is $\Vdash$-enabled by the *whole* sequence. Note that, differently from other event-based models, if C is a configuration, not necessarily a subset of C is a configuration as well (see *e.g.*, $\mathcal{E}_1$ in Fig. 1). This makes it difficult to reason compositionally about configurations, and this is why the notion in Def. 2 below is a little more general than what suggested by our intuition. In an X-*configuration* C, the set C can contain an event e even in the absence of a justification of e through a standard/circular enabling — provided that e belongs to X. This allows, given an X-configuration, to add/remove any event and obtain an Y-configuration, possibly with $Y \neq X$.

Definition 2 (Configuration). *Let* $\mathcal{E} = (E, \#, \vdash, \Vdash)$ *be a CES. For all* $C, X \subseteq E$ *we say that* C *is an* X-configuration *of* $\mathcal{E}$ *iff* $CF(C)$ *and:*

$$\forall e \in C. \ \exists e_0, \dots, e_n \in C. \ e \in \{e_0, \dots, e_n\} \ \wedge$$
$$\forall i \leq n. \, (e_i \in X \ \vee \ \{e_0, \dots, e_{i-1}\} \vdash e_i \ \vee \ \{e_0, \dots, e_n\} \Vdash e_i)$$

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 1. Consider the four CES in Fig. 1.

- $\mathcal{E}_0$ has enablings $\emptyset \vdash a$, $\emptyset \Vdash b$, and conflict $a \# b$. By Def. 2 we have $\emptyset, \{a\}, \{b\} \in \mathcal{F}_{\mathcal{E}_0}$, but $\{a, b\} \notin \mathcal{F}_{\mathcal{E}_0}$.
- $\mathcal{E}_1$ has enablings $\{a\} \vdash b$ and $\{b\} \Vdash a$. Here $\emptyset, \{a, b\} \in \mathcal{F}_{\mathcal{E}_1}$, $\{b\} \in \mathcal{F}_{\mathcal{E}_1}(\{b\})$ and $\{a\} \in \mathcal{F}_{\mathcal{E}_1}(\{a\})$, while neither $\{a\}$ nor $\{b\}$ belong to $\mathcal{F}_{\mathcal{E}_1}(\emptyset)$.
- $\mathcal{E}_2$ has enablings $\{a, b\} \vdash c$, $\{c\} \Vdash a$, and $\{c\} \Vdash b$. The only non-empty configuration of $\mathcal{E}_2$ is $\{a, b, c\}$.
- $\mathcal{E}_3$ has enablings $\{a, b\} \Vdash c$, $\{a, b\} \Vdash d$, $\{c\} \vdash a$, and $\{d\} \vdash b$. We have that $\{a, b, c, d\} \in \mathcal{F}_{\mathcal{E}_3}$. Note that, were one (or both) of the $\Vdash$ turned into a $\vdash$, then the only $\emptyset$-configuration would have been the empty one.
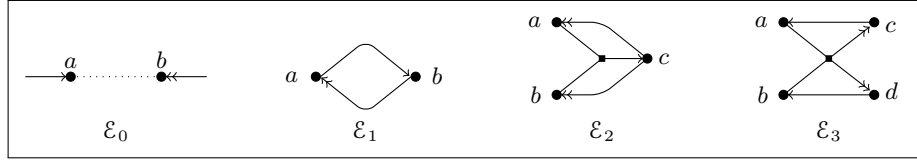
Fig. 1. CES are depicted as directed hypergraphs, where nodes stand for events. An hyperedge from a set of nodes X to node e denotes an enabling $X \circ e$, where $\circ = \vdash$ if the edge has a single arrow, while $\circ = \Vdash$ if the edge has a double arrow. A conflict $a\#b$ is represented by a dotted line between a and b.

We now present some basic properties of CES. Unless stated otherwise, in all the statements below in this section we assume a CES $\mathcal{E} = (E, \#, \vdash, \Vdash)$.

Property 1. For all $C, C', X, Y \subseteq E$ such that $CF(C \cup C')$: (a) $C \in \mathcal{F}(C)$; (b) $X \subseteq Y \implies \mathcal{F}(X) \subseteq \mathcal{F}(Y)$; (c) $C \in \mathcal{F}(X) \wedge C' \in \mathcal{F}(X) \implies C \cup C' \in \mathcal{F}(X)$.

For $\mathcal{A} \subseteq \mathcal{F}(X)$, with $\mathcal{A} \uparrow$ we indicate that there exists $C' \in \mathcal{F}(X)$ such that for all $C \in \mathcal{A}$, $C \subseteq C'$. We say that $\mathcal{A}$ is *finitely compatible*, and write $\mathcal{A} \uparrow^{fin}$, iff $\forall \mathcal{A}_0 \subseteq_{fin} \mathcal{A}. \mathcal{A}_0 \uparrow$.

Property 2 (Finite-completeness). $\mathcal{A} \subseteq \mathcal{F}_{\mathcal{E}}(X) \wedge \mathcal{A} \uparrow^{fin} \implies \bigcup \mathcal{A} \in \mathcal{F}_{\mathcal{E}}(X)$.

Property 3 (Finiteness). $e \in C \in \mathcal{F}(X) \implies \exists C_0 \in \mathcal{F}(X). e \in C_0 \wedge C_0 \subseteq_{fin} C$.

Note that CES do not enjoy *coincidence-freeness*, *i.e.*, it is not always true that:

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

A counterexample to coincidence-freeness is $\mathcal{E}_1$ in Fig. 1, where $\{a, b\} \in \mathcal{F}_{\mathcal{E}_1}$, 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, then each configuration that contains one of them must contain both.

Property 4. For all $C, C', X, Y \subseteq E$ such that $CF(C \cup C')$:

1. $C \in \mathcal{F}(X) \wedge C' \in \mathcal{F}(X \cup C) \implies C \cup C' \in \mathcal{F}(X)$
2. $C \in \mathcal{F}(X) \wedge C' \in \mathcal{F}(X \cup Y) \wedge C \vdash Y \implies C \cup C' \in \mathcal{F}(X)$
3. $C \in \mathcal{F}(X \cup C') \wedge C' \in \mathcal{F}(X \cup Y) \wedge C \Vdash Y \implies C \cup C' \in \mathcal{F}(X)$

3 Relation with logics

We define an encoding of (finite) CES into Propositional Contract Logic (PCL, [4]), an extension of intuitionistic logic which allows for circular reasoning through a "contractual implication" connective. The Hilbert-style axiomatisation of PCL extend that of IPC with the following axioms:

$$\top \twoheadrightarrow \top \qquad (\phi \twoheadrightarrow \phi) \to \phi \qquad (\phi' \to \phi) \to (\phi \twoheadrightarrow \psi) \to (\psi \to \psi') \to (\phi' \twoheadrightarrow \psi')$$

In [4] a proof system is given which enjoys cut elimination and the subformula property; these imply the decidability of the entailment relation $\vdash_{\mathrm{PCL}}$.

In Def. 3 we show a translation from CES into PCL formulae. In particular, our mapping is a bijection into the fragment of PCL which comprises atoms, conjunctions, and non-nested (standard/contractual) implications. For an event structure $\mathcal{E} = \langle E, \#, \vdash, \Vdash \rangle$, we denote with $!E$ the set of events $\{!e \mid e \in E\}$, and we assume $!E$ disjoint from E. For each event in $e \in E \cup !E$, we assume an atom e in the logic. For a set $X \subseteq E$, we write $!X$ for the formula $\bigwedge_{e \in X} !e$.

Definition 3. *Let $\mathcal{E} = \langle E, \#, \vdash, \Vdash \rangle$ be a finite* CES. *The mapping $[\cdot]$ from $\mathcal{E}$ into* PCL *formulae is defined as follows:*

$$[(X_i \circ e_i)_i] = \bigwedge_i [X_i \circ e_i] \qquad [a \# b] = (!a \wedge !b) \to \bot$$

$$[X \circ e] = (!e \wedge X \wedge !X)[\circ] \, e \qquad where \, [\circ] = \begin{cases} \to & if \circ = \vdash \\ \twoheadrightarrow & if \circ = \Vdash \end{cases}$$

Theorem 1. *Let $\mathcal{E}$ be a finite* CES. *Then, for all $C \subseteq E$:*

$$C \in \mathcal{F}_{\mathcal{E}}(X) \iff [\mathcal{E}], !C, X \vdash_{\mathrm{PCL}} C \; and \; [\mathcal{E}], !C \nvdash_{\mathrm{PCL}} \bot$$

Example 2. Consider the CES $\mathcal{E}_2$ from Fig. 1. We have that:

$$[\mathcal{E}_2] = \big((!c \wedge !a \wedge !b \wedge a \wedge b) \to c\big) \wedge \big((!a \wedge !c \wedge c) \twoheadrightarrow a\big) \wedge \big((!b \wedge !c \wedge c) \twoheadrightarrow b\big)$$

Let $C = \{a, b, c\}$. We have that $C \in \mathcal{F}_{\mathcal{E}_2}$, and $[\mathcal{E}_2], !C \vdash_{\mathrm{PCL}} C$. Note that, were the !-ed atoms omitted in the premises of $\to / \twoheadrightarrow$, then we would have, e.g., $[\mathcal{E}_2], !a, !c \vdash_{\mathrm{PCL}} a \wedge c$, from which by Theorem 1 we would have incorrectly deduced that $\{a, c\} \in \mathcal{F}_{\mathcal{E}_2}$.

References

1. M. Abadi and L. Lamport. Composing specifications. *ACM Transactions on Programming Languages and Systems*, 15(1), 1993.
2. M. Abadi and G. D. Plotkin. A logical view of composition. *Theoretical Computer Science*, 114(1), 1993.
3. P. Baldan, A. Corradini, and U. Montanari. Contextual Petri nets, asymmetric event structures, and processes. *Inf. Comput.*, 171(1):1–49, 2001.
4. M. Bartoletti and R. Zunino. A calculus of contracting processes. In *LICS*, 2010.
5. G. Boudol. Flow event structures and flow nets. In *Semantics of Systems of Concurrent Processes*, 1990.
6. P. Maier. Compositional circular assume-guarantee rules cannot be sound and complete. In *FoSSaCS*, 2003.
7. M. Viswanathan and R. Viswanathan. Foundations for circular compositional reasoning. In *ICALP*, 2001.
8. G. Winskel. Event structures. In *Advances in Petri Nets*, pages 325–392, 1986.