Circular causality in event structures

Tiziana Cimoli
Dip. Matematica e Informatica, Università degli Studi di Cagliari
t.cimoli@unica.it

(joint work with M. Bartoletti, G.M. Pinna, R. Zunino)

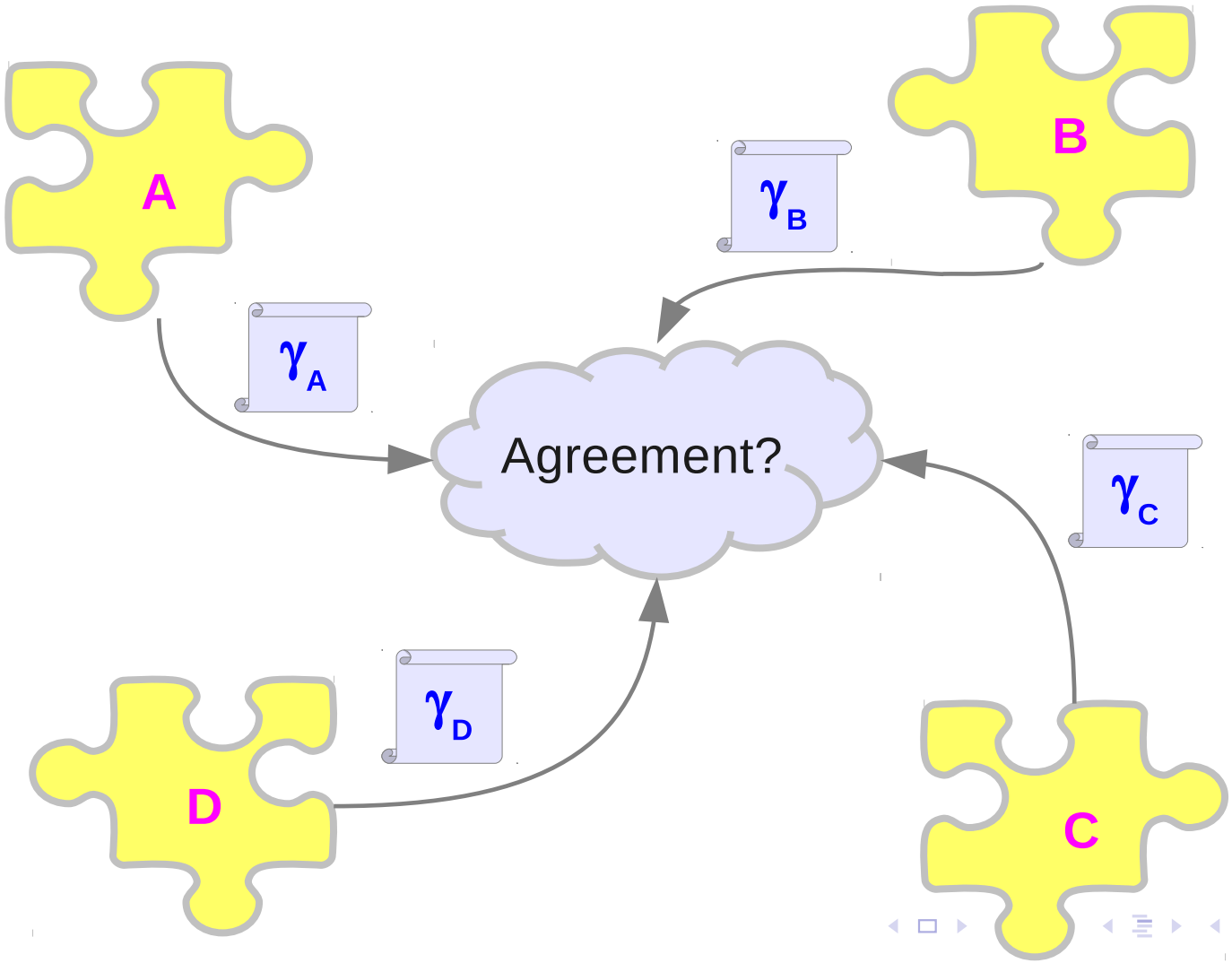
A typical transaction

1. B pays.
2. A ships.

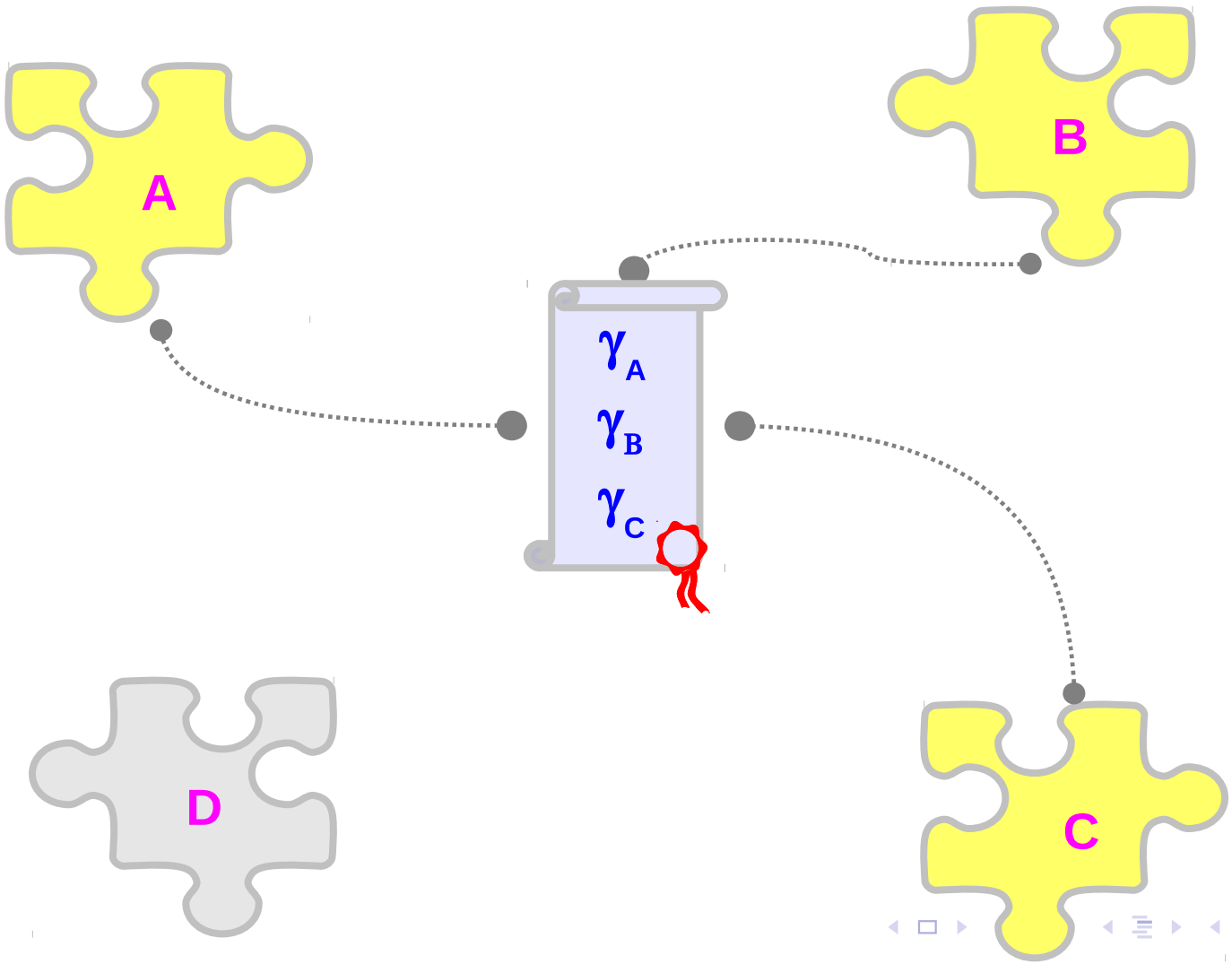
A distrusted transation

1. B pays.
2. A takes the money and runs away.

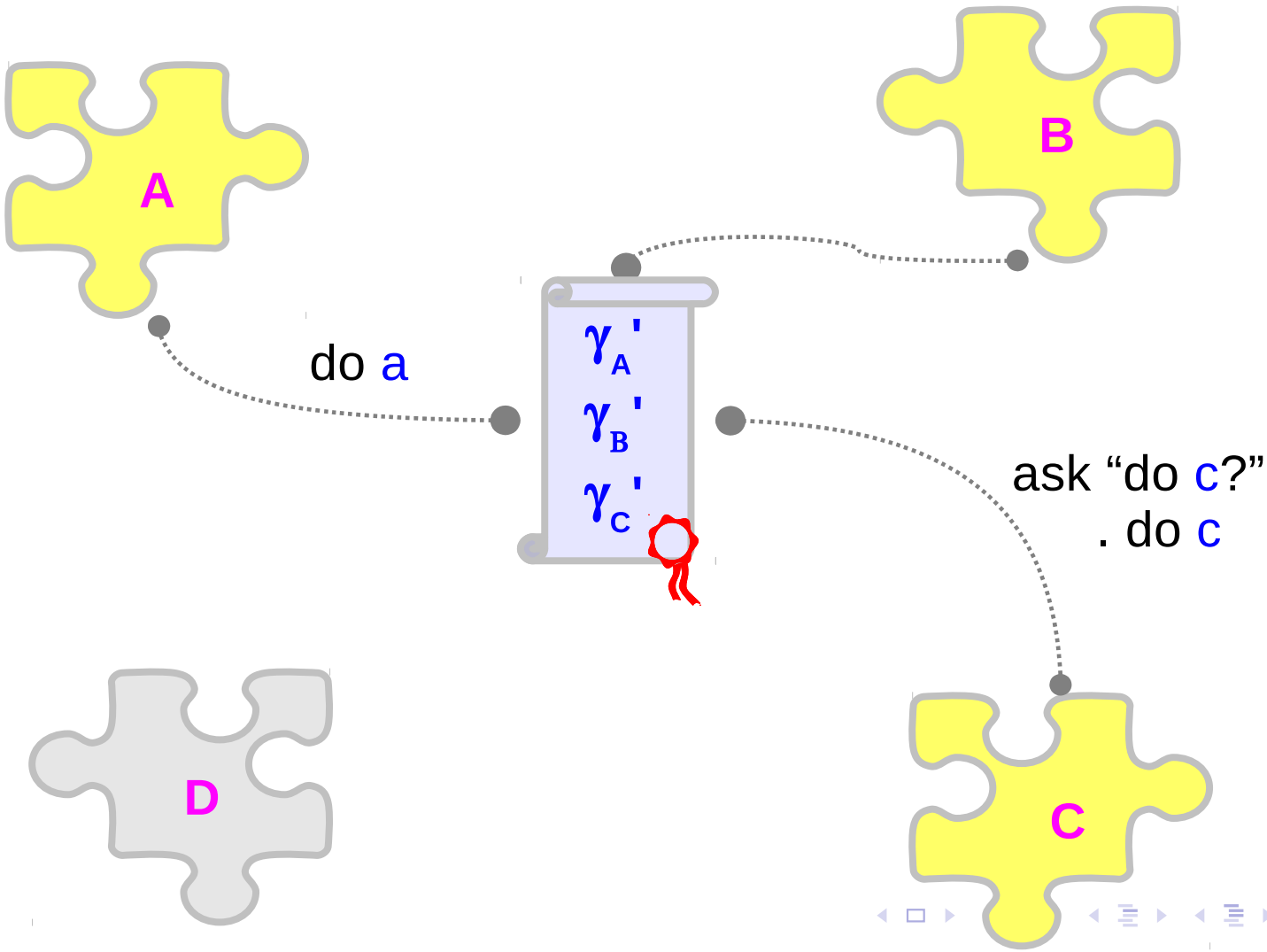
Contract based computing (1)



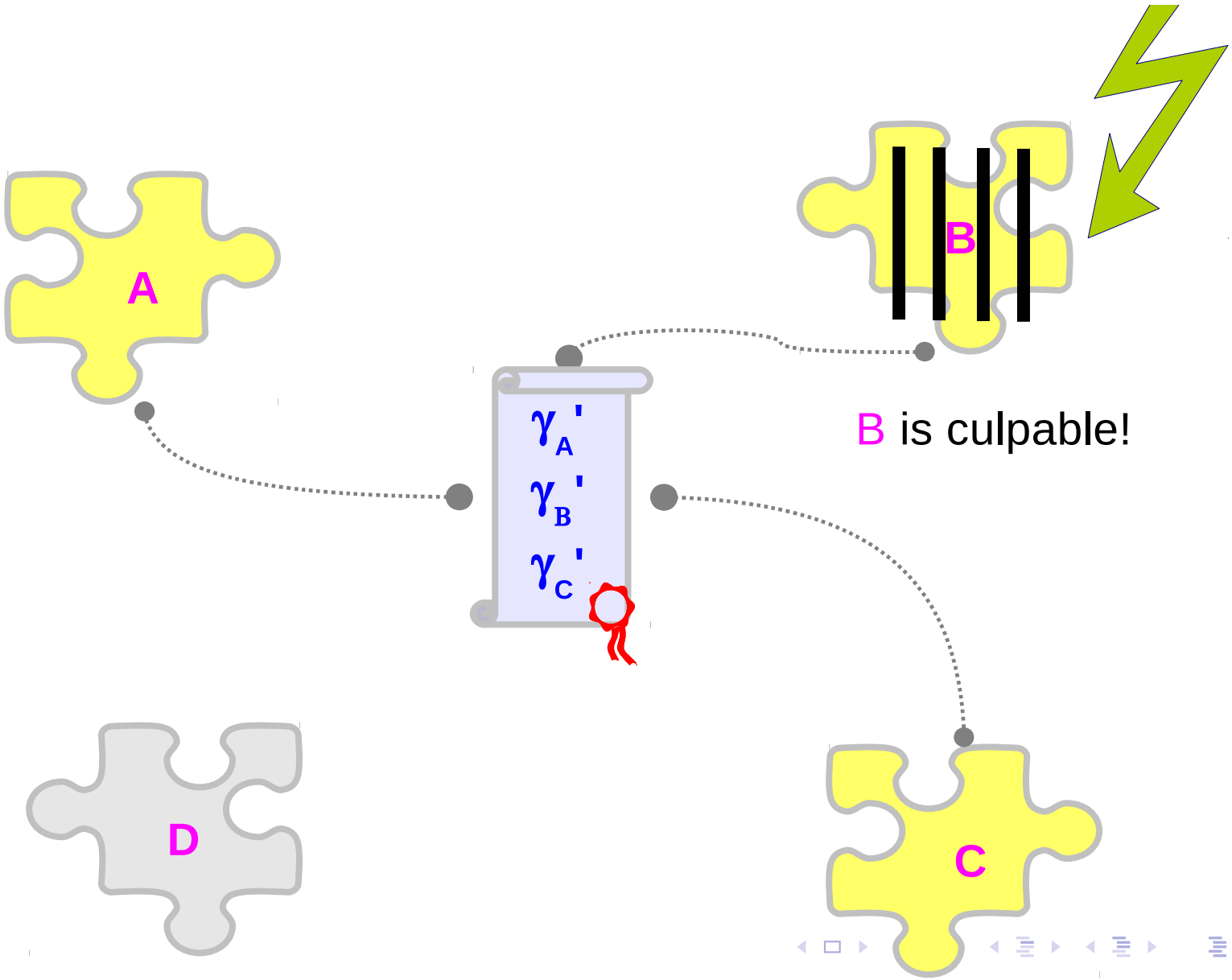
Contract based computing (2)



Contract based computing (3)



Contract based computing (4)



A model for contracts

The model must be able to :

- decide if γ has an agreement
- make γ evolve under actions
- assign duties to principals
- detect violations

Example: "A will ship after B does pay"

- contract-as-process: $\mathsf{pay}.\overline{\mathsf{ship}}$
- contract-as-formula: $\mathsf{pay} \rightarrow \mathsf{ship}$

Winskel's Event structures

Event structures $\mathcal{E} = (E, \#, \vdash)$ are made of:

- a set of events E,
- a conflict relation $\#$ $\quad (e1 \# e2)$
- an enabling relation $\vdash$ $\quad (X \vdash e2)$

ES		Contract
$\{\text{payCC}\} \vdash \text{ship}$		*I will* ship *after you* payCC
$\{\text{payCash}\} \vdash \text{ship}$	$\Longleftrightarrow$	*I will* ship *after you* payCash
$\text{payCash} \# \text{payCC}$		*I will either* payCC *or* payCash

ES: Configurations

A set C of events is a **configuration** if,

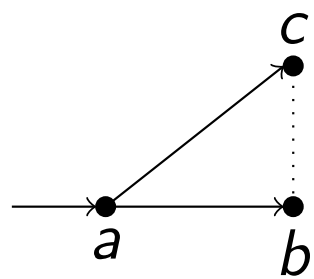
1. C is conflict free and
2. for all $e \in C$, there exists a sequence $\langle e_0, \ldots, e_n \rangle$ of events of C such that $e_n = e$ and:

$$\forall i \leq n : \quad \{e_0, \ldots, e_{i-1}\} \vdash e_i$$

The set of configurations of $\mathcal{E}$ is denoted by $\mathcal{F}_{\mathcal{E}}$.

Example

$\emptyset \vdash \mathsf{a}$
$\{\mathsf{a}\} \vdash \mathsf{b}$
$\{\mathsf{a}\} \vdash \mathsf{c}$
$\mathsf{b} \# \mathsf{c}$



$\mathcal{F} = \{\ \emptyset, \{\mathsf{a}\}, \{\mathsf{a}, \mathsf{b}\}, \{\mathsf{a}, \mathsf{c}\}\}$

Buyer-Seller (1)

1. A says: I ship, after you pay.
2. B says: I pay, after you ship.

Modelled as an event structure:

- $\mathcal{E}_A : \{\text{pay}\} \vdash \text{ship}$
- $\mathcal{E}_B : \{\text{ship}\} \vdash \text{pay}$

The event structure $\mathcal{E}_A \cup \mathcal{E}_b$ does not have any configuration besides the empty one:

- no agreement and no move !

Buyer-Seller (2)

1. A says: I ship, after you pay.
2. B says: I pay.

Modelled as an event structure:

- $\mathcal{E}_A : \{\text{pay}\} \vdash \text{ship}$
- $\mathcal{E}_B : \emptyset \vdash \text{pay}$

Configurations of $\mathcal{E}_A \cup \mathcal{E}_b$ are : $\emptyset, \{\text{pay}\}$ and $\{\text{pay}, \text{ship}\}$. On $\{\text{pay}, \text{ship}\}$ there is an agreement.

Buyer-seller: the attack (3)

Now, an attack is possible:

1. M(A) says: 1 sheep, after you pay
2. B says: I pay.

Modelled as an event structure:

- $\mathcal{E}_M$: $\{\text{pay}\} \vdash \text{sheep}$
- $\mathcal{E}_B$: $\emptyset \vdash \text{pay}$

The problem: a contract of the form $\emptyset \vdash a$ offers no protection.

The idea.

1. M(A) says: 1 sheep, after you pay
2. B says: I will pay if you *promise* to ship.

Modelled as an event structure:

- $\mathcal{E}_A : \{\text{pay}\} \vdash \text{sheep}$.
- $\mathcal{E}_B : \{\text{ship}\} \Vdash \text{pay}$.

Now, B is protected.

Event structures with circular causality

CES $\mathcal{E} = (E, \#, \vdash, \Vdash)$ are made of:

- a set of events E,
- a conflict relation $\#$,
- an enabling relation $\vdash$,
- a circular enabling relation $\Vdash$.

CES:		Contract:
$\{\text{pay}\} \vdash \text{ship}$ $\{\text{ship}\} \Vdash \text{pay}$	$\Longleftrightarrow$	*I will* ship *after you* pay. *I will* pay *if you promise to* ship.

Event structures with circular causality

CES $\mathcal{E} = (E, \#, \vdash, \Vdash)$ are made of:

- a set of events E,
- a conflict relation $\#$,
- an enabling relation $\vdash$,
- a circular enabling relation $\Vdash$.

CES:		Contract:
$\{\text{pay}\} \Vdash \text{ship}$ $\{\text{ship}\} \Vdash \text{pay}$	$\Longleftrightarrow$	*I will* ship *if you promise to* pay. *I will* pay *if you promise to* ship.

CES: configurations

Winskel's configurations:

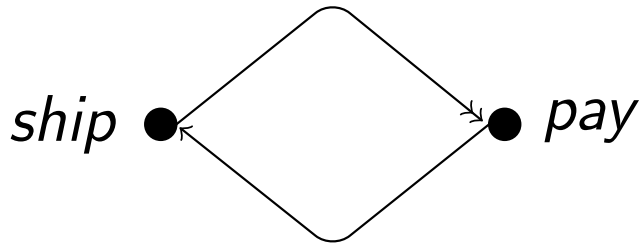
$$\forall i \leq n : \quad \{e_0, \ldots, e_{i-1}\} \vdash e_i$$

CES configurations:

$$\forall i \leq n : \quad \{e_0, \ldots, e_{i-1}\} \vdash e_i \ \vee \ \{e_0, \ldots, e_n\} \Vdash e_i$$

CES: example

$\mathsf{pay} \vdash \mathsf{ship}$
$\mathsf{ship} \nvdash \mathsf{pay}$



Configurations:

- $\emptyset$
- $\{\mathsf{ship}, \mathsf{pay}\}$ has only the trace $\langle \mathsf{pay}, \mathsf{ship} \rangle$

ES: families of configurations

The set $\mathcal{F}$ of configurations of an ES satisfies:

- **coherence**:
  for all $\mathcal{A} \subseteq \mathcal{F}$ pairwise compatible[1] $\implies \bigcup \mathcal{A} \in \mathcal{F}$

[1] $\mathcal{A} \subseteq \mathcal{F}$ **pairwise compatible** iff $\forall e, e' \in \bigcup \mathcal{A}. \Box\exists C \in \mathcal{F}. e, e' \in C$

ES: families of configurations

The set $\mathcal{F}$ of configurations of an ES satisfies:

- **coherence**:
  for all $\mathcal{A} \subseteq \mathcal{F}$ pairwise compatible[1] $\implies \bigcup \mathcal{A} \in \mathcal{F}$

- **finiteness**:
  $\forall C \in \mathcal{F}.\ \forall e \in C.\ \exists C_0 \in \mathcal{F}.\ e \in C_0 \subseteq_{fin} C$

[1] $\mathcal{A} \subseteq \mathcal{F}$ **pairwise compatible** iff $\forall e, e' \in \bigcup \mathcal{A}.\ \exists C \in \mathcal{F}.\ e, e' \in C$

ES: families of configurations

The set $\mathcal{F}$ of configurations of an ES satisfies:

- **coherence**:
  for all $\mathcal{A} \subseteq \mathcal{F}$ pairwise compatible[1] $\implies \bigcup \mathcal{A} \in \mathcal{F}$
- **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**:
  for all $C \in \mathcal{F}$, and for all $e \neq e' \in C$:
  $\exists C' \in \mathcal{F}.\ C' \subseteq C \ \wedge\ (e \in C' \iff e' \notin C')$

[1] $\mathcal{A} \subseteq \mathcal{F}$ **pairwise compatible** iff $\forall e, e' \in \bigcup \mathcal{A}.\ \exists C \in \mathcal{F}.\ e, e' \in C$

CES: quasi-families of configurations

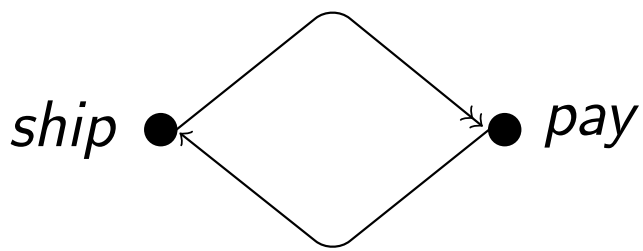
The set $\mathcal{F}$ of configurations of a CES form a quasi-family of subsets of events because it satisfies

- coherence and
- finiteness

... but in general it does not satisfy coincidence-freeness!

Example

pay $\vdash$ ship
ship $\nVdash$ pay
$\mathcal{F} = \{\emptyset, \{\text{pay}, \text{ship}\}\}$



From Quasi-families to CES

Theorem.

For all quasi-families of configurations $\mathcal{F}$, there exists a CES $\hat{\mathcal{E}}$ (with circular enablings only) such that

$$\mathcal{F}_{\hat{\mathcal{E}}} = \mathcal{F}$$

ES: LTS

Winksel's LTS:

$$\frac{C \vdash e \qquad CF(C \cup \{e\})}{C \xrightarrow{e}_{\varepsilon} C \cup \{e\}}$$

Ex: $\vdash a, \quad \{a\} \vdash b$ $\qquad\qquad \emptyset \xrightarrow{a} \{a\} \xrightarrow{b} \{a, b\}$

What happens in CES?

Ex: $\{b\} \nvdash a, \quad \{a\} \vdash b$ $\qquad\qquad \emptyset \xrightarrow{a} \; ? \; \xrightarrow{b} \{a, b\}$

CES: X-configurations

CES Configurations:

$$\{e_0, \ldots, e_{i-1}\} \vdash e_i \quad \vee \quad \{e_0, \ldots, e_n\} \Vdash e_i$$

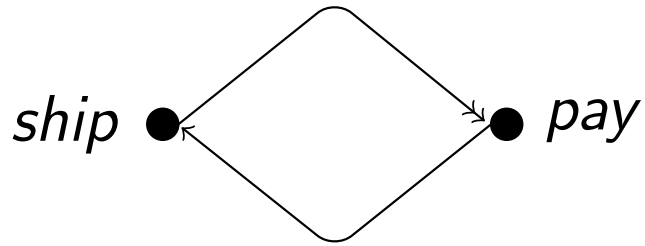
CES X-configurations:

$$\{e_0, \ldots, e_{i-1}\} \vdash e_i \quad \vee \quad \{e_0, \ldots, e_n\} \Vdash e_i \quad \vee \quad e_i \in X$$

The set of all X-configurations is denoted by $\mathcal{F}(X)$.
X is a superset of all the pending credits.

Example

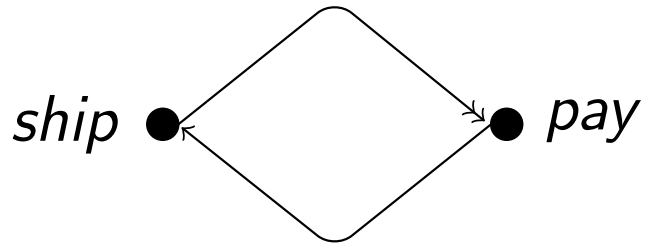
$\mathsf{pay} \vdash \mathsf{ship}$
$\mathsf{ship} \nvdash \mathsf{pay}$



$$(\emptyset, \emptyset) \xrightarrow{\mathsf{a}} \{\{\mathsf{a}\}, \{\mathsf{a}\}\} \xrightarrow{\mathsf{b}} \{\{\mathsf{a}, \mathsf{b}\}, \emptyset\}$$

Example

$\mathsf{pay} \vdash \mathsf{ship}$
$\mathsf{ship} \nvdash \mathsf{pay}$



$$\begin{array}{ccccc} (\emptyset, \emptyset) & \xrightarrow{\mathsf{a}} & \{\{\mathsf{a}\}, \{\mathsf{a}\}\} & \xrightarrow{\mathsf{b}} & \{\{\mathsf{a}, \mathsf{b}\}, \emptyset\} \\ | & & | & & | \\ \mathcal{F}(\emptyset) & & \mathcal{F}(\{a\}) & & \mathcal{F}(\emptyset) \end{array}$$

LTS for event structures

Winksel's LTS:

$$\frac{C \vdash e \qquad CF(C \cup \{e\})}{C \xrightarrow{e}_{\varepsilon} C \cup \{e\}}$$

CES' LTS:

$$\frac{CF(C \cup \{e\})}{(C, X) \xrightarrow{e}_{\varepsilon} (C \cup \{e\}, X')}$$

where $X' =$ least credit of $C \cup \{e\}$

Properties of X-configurations (1)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X) \qquad C' \in \mathcal{F}(X \cup C)}{C \cup C' \in \mathcal{F}(X)}$$

Properties of X-configurations (1)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X) \qquad C' \in \mathcal{F}(X \cup C)}{C \cup C' \in \mathcal{F}(X)}$$

In Intuitionistic Propositional Logic:

$$\frac{\Gamma \vdash p \qquad \Gamma,\ p \vdash q}{\Gamma \vdash q}\ (\textsc{Cut})$$

Properties of X-configurations (2)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X) \qquad C' \in \mathcal{F}(X \cup Y) \qquad C \vdash Y}{C \cup C' \in \mathcal{F}(X)}$$

Properties of X-configurations (2)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X) \qquad C' \in \mathcal{F}(X \cup Y) \qquad C \vdash Y}{C \cup C' \in \mathcal{F}(X)}$$

In Intuitionistic Propositional Logic:

$$\frac{\Gamma \vdash p \qquad \Gamma, q \vdash r \qquad p \to q \in \Gamma}{\Gamma \vdash r}\ (\to\mathrm{L})$$

Other properties of X-configurations (3)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X \cup C') \qquad C' \in \mathcal{F}(X \cup Y) \qquad C \Vdash Y}{C \cup C' \in \mathcal{F}(X)}$$

Other properties of X-configurations (3)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X \cup C') \qquad C' \in \mathcal{F}(X \cup Y) \qquad C \Vdash Y}{C \cup C' \in \mathcal{F}(X)}$$

$$\frac{\Gamma, r \vdash p \qquad \Gamma, q \vdash r \qquad p \twoheadrightarrow q \in \Gamma}{\Gamma \vdash r}\ (\textsc{Fix})$$

Other properties of X-configurations (3)

Th. If $CF(C \cup C')$:

$$\frac{C \in \mathcal{F}(X \cup C') \qquad C' \in \mathcal{F}(X \cup Y) \qquad C \Vdash Y}{C \cup C' \in \mathcal{F}(X)}$$

$$\frac{\Gamma, r \vdash p \qquad \Gamma, q \vdash r \qquad p \twoheadrightarrow q \in \Gamma}{\Gamma \vdash r}\ (\textsc{Fix})$$

Propositional Contract Logic (PCL) - M. Bartoletti & R. Zunino, LICS'10

Propositional Contract Logic

(M. Bartoletti & R. Zunino, LICS'10)

Syntax: $p ::= \text{IPC formulae} \mid p \twoheadrightarrow p$

Axioms:

IPC axioms $+$ some for the contractual implications:

$\top \twoheadrightarrow \top$

$(p \twoheadrightarrow p) \to p$

$(p' \to p) \to (p \twoheadrightarrow q) \to (q \to q') \to (p' \twoheadrightarrow q')$

Note: $a \twoheadrightarrow b \ \wedge \ b \twoheadrightarrow a \ \vdash_{PCL} \ a \ \wedge \ b$

Structural properties of PCL

Gentzen-style proof system $\vdash_{\mathsf{PCL}}$:

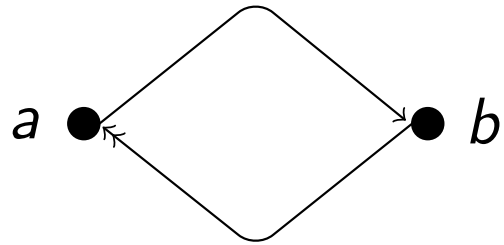
- consistency
- subformula property
- cut elimination
- decidability

PCL not homomorphically encodable into IPC.

CES configuration via PCL

$[]_{\mathcal{F}}$: finite CES $\longrightarrow$ PCL formulae

$\mathsf{a} \vdash \mathsf{b}$
$\mathsf{b} \Vdash \mathsf{a}$



Encoding of $\mathcal{E}$:

- $[\mathsf{a} \vdash \mathsf{b}]_{\mathcal{F}} = (!b \wedge !a \wedge a) \rightarrow b$
- $[\mathsf{b} \Vdash \mathsf{a}]_{\mathcal{F}} = (!a \wedge !b \wedge b) \twoheadrightarrow a$

$$\{\mathsf{a}, \mathsf{b}\} \in \mathcal{F} \iff [\mathcal{E}]_{\mathcal{F}}, !a, !b \vdash_{\mathsf{PCL}} a \wedge b$$
$$\{\mathsf{a}\} \notin \mathcal{F} \iff [\mathcal{E}]_{\mathcal{F}}, !a \nvdash_{\mathsf{PCL}} a$$

CES configuration via PCL

Def.

$$
\begin{aligned}
[(X_i \circ e_i)_{i\in I}]_{\mathcal{F}} &= \{[X_i \circ e_i]_{\mathcal{F}} \mid i \in I\} \\
[X \circ e]_{\mathcal{F}} &= \big(!e \wedge X \wedge !X\big)[\circ]\ e \\
[a \# b]_{\mathcal{F}} &= (!a \wedge !b) \to \bot
\end{aligned}
\qquad
[\circ] = \begin{cases} \to & \text{if } \circ = \vdash \\ \twoheadrightarrow & \text{if } \circ = \Vdash \end{cases}
$$

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

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

Conclusions

- A model for contracts that
  - is a conservative extension of event structures
  - offers both agreements and protection

Conclusions

- A model for contracts that
  - is a conservative extension of event structures
  - offers both agreements and protection
- Strong relations between CES and contract logic
  - configurations,
  - reachable events
  - *urgent* events

Conclusions

- A model for contracts that
  - is a conservative extension of event structures
  - offers both agreements and protection
- Strong relations between CES and contract logic
  - configurations,
  - reachable events
  - *urgent* events
- There is a lot of work to do:
  - deeper understanding of the structure of configurations
  - game-theoretic notions of protection and agreement
  - relations with Petri nets
  - ...

Thanks!

Urgent events

Def. We say that e is **urgent** in (C, X) iff

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

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

Theo. Let (C, X) be a reachable state of $\rightharpoonup_{\mathcal{U}_{\mathcal{E}}}$. Then:

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

Urgent events via PCL

Def. For a finite, conflict-free CES $\mathcal{E}$, we define the accessibility relation $\rightarrow_{[\mathcal{E}]_{\mathcal{U}}}$ of an LTS as follows:

$$C \xrightarrow{e}_{[\mathcal{E}]_{\mathcal{U}}} C \cup \{e\} \quad \text{iff} \quad [\mathcal{E}]_{\mathcal{U}}, !C \vdash_{\mathsf{PCL}} Ue \ \wedge \ !C \not\vdash_{\mathsf{PCL}} !e$$

Th. For a finite, conflict-free CES $\mathcal{E}$, $\rightarrow_{\mathcal{U}_{\mathcal{E}}} = \rightarrow_{[\mathcal{E}]_{\mathcal{U}}}$

urgency (what to do and when) can be characterized using the encoding

The Gentzen-style rules for PCL

$$\frac{\Gamma \vdash q}{\Gamma \vdash p \twoheadrightarrow q}\ (\textsc{Zero})$$

$$\frac{\Gamma,\ p \twoheadrightarrow q,\ a \vdash p \quad \Gamma,\ p \twoheadrightarrow q,\ q \vdash b}{\Gamma,\ p \twoheadrightarrow q \vdash a \twoheadrightarrow b}\ (\textsc{PrePost})$$

$$\frac{\Gamma,\ p \twoheadrightarrow q,\ r \vdash p \quad \Gamma,\ p \twoheadrightarrow q,\ q \vdash r}{\Gamma,\ p \twoheadrightarrow q \vdash r}\ (\textsc{Fix})$$