Contract Agreements via Logic

Massimo Bartoletti

(joint work with T. Cimoli, P. Di Giamberardino, and R. Zunino)

University of Cagliari

June 6, 2013

A Calculus of Contracting Processes

Massimo Bartoletti
Dipartimento di Matematica e Informatica
Università degli Studi di Cagliari
Email: bart@unica.it

Roberto Zunino
Dipartimento di Ingegneria e Scienza dell'Informazione
Università degli Studi di Trento
Email: zunino@disi.unitn.it

***Abstract*—We propose a formal theory of contract-based computing. We model contracts as formulae in an intuitionistic logic extended with a "contractual" form of implication. Decidability holds for our logic: this allows us to mechanically infer the rights and the duties deriving from any set of contracts. We embed our logic in a core calculus of contracting processes, which combines features from concurrent constraints and calculi for multiparty sessions, while subsuming several idioms for concurrency.**

***Keywords*-contracts; circular assume-guarantee; concurrent constraints; cut elimination**

I. Introduction

In Web transactions, the typical dynamics is that a client chooses a service provider that she trusts, relying on the fact that the service implements the required features. Such features are typically written in a "service level agreement" (SLA). Although this document is legally binding, it is not a formal specification. Formalising it would be desirable, for two main reasons. First, a formal SLA could be exploited by the client to mechanize the search of a service meeting her requests. Second, in the case the provider does not honour its SLA, automatic means could be devised to resolve the dispute. This would be more practical than taking legal steps against the provider, especially for transactions dealing with small amounts of money.

The interaction among parties has then to be regulated by a suitable *contract*, which formally subordinates the duties of a client to the duties of a service, and *vice versa*. The crucial problems are how to model a contract, how to infer when a set of contracts gives rise to an agreement among the stipulating parties, and how to single out the responsible of a possible violation.

An example: To give the intuition about our contracts, suppose there are two kids: Alice, who has a toy airplane, and Bob, who has a bike. Before sharing their toys, the two kids stipulate the following "gentlemen's agreement":

Alice: I will lend my airplane to you, Bob, provided that I borrow your bike.
Bob: I will lend my bike to you, Alice, provided that I borrow your airplane.

Let us write a for the atomic proposition "Alice lends her airplane" and b for "Bob lends his bike". A (wrong) formalisation of the above contracts in classical logic could model Alice's contract A as $\mathsf{b} \rightarrow \mathsf{a}$, and Bob's B as $\mathsf{a} \rightarrow \mathsf{b}$. However, from this we cannot deduce the expected agreement, i.e. $A \land B \rightarrow \mathsf{a} \land \mathsf{b}$ does not hold. To solve this issue, we propose Propositional Contract Logic (PCL), that extends intuitionistic logic IPC with a *contractual implication* connective $\twoheadrightarrow$. In PCL we have the desired agreement:

$$(\mathsf{b} \twoheadrightarrow \mathsf{a}) \;\land\; (\mathsf{a} \twoheadrightarrow \mathsf{b}) \;\rightarrow\; \mathsf{a} \land \mathsf{b}$$

To put our contracts at work, we introduce a process calculus which embeds our logic. This calculus belongs to the family of concurrent constraints [1], using PCL formulae as constraints. A process can assert a constraint c (a PCL formula) through the primitive $\mathsf{tell}\, c$. For instance, the following process models Alice exposing her contract:

$$(x)\ \mathsf{tell}\,\mathsf{b}(x) \twoheadrightarrow \mathsf{a}(x)$$

Formally, this will add $\mathsf{b}(x) \twoheadrightarrow \mathsf{a}(x)$ to the set of constraints. The formal parameter x represents the identifier of the actual session to be established between Alice and Bob. As it happens for sessions centered calculi [2], [3], sessions are an important aspect also in our calculus, since they allow for distinguishing among different instantiations of the same contract. The outer (x) is a scope delimitation for the variable x, similarly to the Fusion calculus [4].

After having exposed her contract, Alice will wait until finding that she has actually to lend her airplane to Bob. This is modelled as $\mathsf{fuse}_x\, \mathsf{a}(x)$. The primitive $\mathsf{fuse}_x\, c$ implements a contract-based multiparty agreement. To do that, it checks the entailment of the constraint c, and binds the variable x to an actual session identifier, shared among all the parties involved in the contract. So, we will model Alice as:

$$\mathit{Alice} = (x)\ \big(\mathsf{tell}\,\mathsf{b}(x) \twoheadrightarrow \mathsf{a}(x).\ \mathsf{fuse}_x\,\mathsf{a}(x).\ \mathit{lendAirplane}\big)$$

where the process $\mathit{lendAirplane}$ (no further specified) models Alice actually lending her airplane to Bob. The overall behaviour of Alice is then: *(i)* issue the contract; *(ii)* wait until discovering the duty of lending the airplane; *(iii)* finally, lend the airplane. Dually, we model Bob as follows:

$$\mathit{Bob} = (y)\ \big(\mathsf{tell}\,\mathsf{a}(y) \twoheadrightarrow \mathsf{b}(y).\ \mathsf{fuse}_y\,\mathsf{b}(y).\ \mathit{lendBike}\big)$$

LICS'10

A theory of agreements and protection

Massimo Bartoletti[1], Tiziana Cimoli[1], and Roberto Zunino[2]

[1] Università degli Studi di Cagliari, Italy
[2] Università di Trento and COSBI, Italy

Abstract. We present a theory of contracts. Contracts are interacting processes with an explicit notion of obligations and objectives. We model processes and their obligations as event structures. We define a general notion of *agreement*, by interpreting contracts as multi-player concurrent games. A participant agrees on a contract if she has a strategy to reach her objectives (or make another participant chargeable for a violation), whatever the moves of her adversaries. We then tackle the problem of *protection*. A participant is protected by a contract when she has a strategy to defend herself in all possible contexts, even in those where she has not reached an agreement. We show that, in a relevant class of contracts, agreements and protection mutually exclude each other. We then propose a novel formalism for modelling contractual obligations: event structures with circular causality. Using this model, we show how to construct contracts which guarantee both agreements and protection.

1 Introduction

The lack of precise guarantees about the reliability and security of cloud services is a main deterrent for industries wishing to move their applications and business to the cloud [1]. A key problem is how to drive safe and fair interactions among distributed participants which are possibly mutually distrusted, and have possibly conflicting individual goals. In addition to the well-known difficulties of distributed software systems (distribution, concurrency, heterogeneity, mobility, *etc.*), cloud components and infrastructures are often under the governance of different providers, possibly competing among each other. Analysis and verification techniques can be applied only on the software components under one's control, while no assumptions can be made about the components made available by other providers. Therefore, standard compositional techniques have to be adapted to cope with the situation where providers fail to keep the promises made, or even choose not to.

We envision a *contract-oriented computing* paradigm [3], where reliable interactions are driven by contracts which formalise Service-Level Agreements. Contracts specify the behavior of a software component, from the point of view of the interactions it may participate in, and the goals it tries to reach. Differently from most of the approaches based on behavioural types [15], which use contracts only in the "matchmaking" phase, a contract-oriented component is not supposed to be *honest*, in that it may not keep the promises made.

POST'13

Propositional Contract Logic
(Bartoletti & Zunino, LICS'10)

PCL = IPC + contractual implication $p \twoheadrightarrow q$

$$\frac{\Delta \vdash p \twoheadrightarrow q \quad \Delta, q \vdash p}{\Delta \vdash q} \; (\twoheadrightarrow \mathrm{E})$$

$$\frac{\Delta \vdash q}{\Delta \vdash p \twoheadrightarrow q} \; (\twoheadrightarrow \mathrm{I1}) \qquad \frac{\Delta \vdash p' \twoheadrightarrow q' \qquad \begin{array}{ll} \Delta, p & \vdash p' \\ \Delta, q' & \vdash p \twoheadrightarrow q \end{array}}{\Delta \vdash p \twoheadrightarrow q} \; (\twoheadrightarrow \mathrm{I2})$$

PCL

Assume A and B declare the contracts:

- A says: $b \rightarrow a$
- B says: $a \rightarrow b$

Do they reach an **agreement**?

$$\dfrac{\Delta \vdash b \rightarrow a \quad \dfrac{\Delta \vdash a \rightarrow b \quad \dfrac{\vdots}{\Delta \vdash a}}{\Delta \vdash b}\,(\rightarrow\mathrm{E})}{\Delta \vdash a}\,(\twoheadrightarrow\mathrm{E})$$

No agreement!

PCL

A changes her contract:

- A says: $b \twoheadrightarrow a$
- B says: $a \rightarrow b$

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

Agreement: $(b \twoheadrightarrow a) \wedge (a \rightarrow b) \vdash a \wedge b$

PCL

A changes her contract again:

- A says: a
- B says: $a \to b$

Of course we have an agreement:

$$\begin{aligned} a \wedge (a \to b) \quad & \to \quad (b \twoheadrightarrow a) \wedge (a \to b) \\ & \to \quad a \wedge b \end{aligned}$$

but, intuitively, A is not **“protected”**

A theory of agreements and protection
(Bartoletti, Cimoli & Zunino, POST'13)

Contracts = Obligations + Objectives

- Obligations = Event Structures
  - a set of events E,
  - a conflict relation $\#$
  - an enabling relation $\vdash$
- Objectives = functions Φ over sequences of events

Example:

- A's obligations: $\vdash a$ ☺ if $b \in \overline{\sigma}$ ☹ if $a \in \overline{\sigma}$, $b \notin \overline{\sigma}$
- B's obligations: $\{a\} \vdash b$ ☺ if $a \in \overline{\sigma}$ ☹ if $b \in \overline{\sigma}$, $a \notin \overline{\sigma}$

A theory of agreements and protection

(Bartoletti, Cimoli & Zunino, POST'13)

Contracts = Obligations + Objectives

- Obligations = Event Structures
  - a set of events E,
  - a conflict relation $\#$
  - an enabling relation $\vdash$
- Objectives = functions Φ over sequences of events

Example:

- A's obligations: $\vdash a$ ☺ if $b \in \overline{\sigma}$ ☹ if $a \in \overline{\sigma}$, $b \notin \overline{\sigma}$
- B's obligations: $\{a\} \vdash b$ ☺ if $a \in \overline{\sigma}$ ☹ if $b \in \overline{\sigma}$, $a \notin \overline{\sigma}$

Contracts as games

A **play** is a trace σ of the LTS defined by:

$$\frac{C \vdash e \qquad e \notin C \qquad C \cup \{e\} \text{ conflict-free}}{C \xrightarrow{e} C \cup \{e\}}$$

A **strategy** Σ for A associates each finite play σ to set of events of A, such that

$$e \in \Sigma(\sigma) \implies \sigma e \text{ is a play}$$

Winning strategies

A participant A is **innocent** in σ iff:

$$\forall i \geq 0.\ \forall e \text{ of A}.\ \left(\overline{\sigma_i} \xrightarrow{e} \implies \exists j \geq i.\ \overline{\sigma_j} \not\xrightarrow{e}\right)$$

A **wins** in σ iff $\mathcal{W}\text{A}\sigma = ☺$, where

$$\mathcal{W}\text{A}\sigma = \begin{cases} \Phi\text{A}\sigma & \text{if all participants are innocent in } \sigma \\ ☹ & \text{if A is culpable in } \sigma \\ ☺ & \text{otherwise} \end{cases}$$

Σ is a **winning strategy** for A in $\mathcal{C}$ iff A wins in every fair play of $\mathcal{C}$ which conforms to Σ.

Winning strategies

A participant A is **innocent** in σ iff:

$$\forall i \geq 0.\ \forall e \text{ of A}.\ \left(\overline{\sigma_i} \xrightarrow{e} \implies \exists j \geq i.\ \overline{\sigma_j} \not\xrightarrow{e}\right)$$

A **wins** in σ iff $\mathcal{W}\text{A}\sigma = ☺$, where

$$\mathcal{W}\text{A}\sigma = \begin{cases} \Phi\text{A}\sigma & \text{if all participants are innocent in } \sigma \\ ☹ & \text{if A is culpable in } \sigma \\ ☺ & \text{otherwise} \end{cases}$$

Σ is a **winning strategy** for A in $\mathcal{C}$ iff A wins in every fair play of $\mathcal{C}$ which conforms to Σ.

Winning strategies

A participant A is **innocent** in σ iff:

$$\forall i \geq 0.\ \forall e \text{ of } A.\ \left(\overline{\sigma_i} \xrightarrow{e} \implies \exists j \geq i.\ \overline{\sigma_j} \not\xrightarrow{e}\right)$$

A **wins** in σ iff $\mathcal{W} A \sigma = ☺$, where

$$\mathcal{W} A \sigma = \begin{cases} \Phi A \sigma & \text{if all participants are innocent in } \sigma \\ ☹ & \text{if A is culpable in } \sigma \\ ☺ & \text{otherwise} \end{cases}$$

Σ is a **winning strategy** for A in $\mathcal{C}$ iff A wins in every fair play of $\mathcal{C}$ which conforms to Σ.

Contracts as games — an example

$A : \vdash a, \ \vdash a', \ a \# a'$

A : ☺ if $b \in \overline{\sigma}$ or $c \in \overline{\sigma}$

$B : \ a \vdash b, \ a \vdash c, \ b \# c$

B : ☺ if $a \in \overline{\sigma}$, 😐 if $b, c \notin \overline{\sigma}$

Contracts as games — an example

$A : \vdash a,\ \vdash a',\ a \# a'$

$B :\ a \vdash b,\ a \vdash c,\ b \# c$

A : ☺ if $b \in \overline{\sigma}$ or $c \in \overline{\sigma}$

B : ☺ if $a \in \overline{\sigma}$, 😐 if $b, c \notin \overline{\sigma}$

$$\Sigma_A(\sigma) = \begin{cases} \{a\} & \text{if } \sigma = \varepsilon \\ \emptyset & \text{if } \sigma \neq \varepsilon \end{cases}$$

$$\Sigma_B(\sigma) = \begin{cases} \{b\} & \text{if } a \in \overline{\sigma} \\ \emptyset & \text{if } a \notin \overline{\sigma} \end{cases}$$

Contracts as games — an example

$A : \vdash a,\ \vdash a',\ a \# a'$

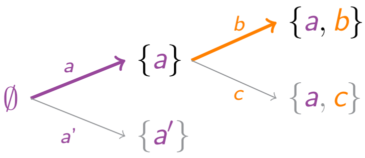
$B : \ a \vdash b,\ a \vdash c,\ b \# c$

A : ☺ if $b \in \overline{\sigma}$ or $c \in \overline{\sigma}$

B : ☺ if $a \in \overline{\sigma}$, 😐 if $b, c \notin \overline{\sigma}$

$$\Sigma_A(\sigma) = \begin{cases} \{a\} & \text{if } \sigma = \varepsilon \\ \emptyset & \text{if } \sigma \neq \varepsilon \end{cases}$$

$$\Sigma_B(\sigma) = \begin{cases} \{b\} & \text{if } a \in \overline{\sigma} \\ \emptyset & \text{if } a \notin \overline{\sigma} \end{cases}$$



	A		B	
$\langle\ \rangle$	😈	☹	😇	☺
$\langle a' \rangle$	😇	☹	😇	😐
$\langle a \rangle$	😇	☺	😈	☹
$\langle a\ b \rangle$	😇	☺	😇	☺
$\langle a\ c \rangle$	😇	☺	😇	☺

Agreement & Protection

- $\mathcal{C}$ admits an **agreement** iff

  all the participants have a winning strategy in $\mathcal{C}$.

- $\mathcal{C}$ **protects** A iff

  $\forall \mathcal{C}'$ compatible with $\mathcal{C}$,

  A has a non-losing strategy in $\mathcal{C} \mid \mathcal{C}'$.

Protection is relevant when service brokers are untrusted!

Agreement *vs.* Protection

Theorem. Let $\mathcal{C}_1, \ldots, \mathcal{C}_n$ be contracts with circular payoffs. Then:

EITHER

$\mathcal{C}_1 \mid \cdots \mid \mathcal{C}_n$ admits an agreement

OR

all the participants are protected

Extends a result in: Even and Jacobi. Relations among public key signature system, 1980.

Event structures with circular causality

CES = ES + circular enabling relation $\Vdash$

Plays $\sigma = e_0\, e_1\, e_2 \cdots$ are traces of the LTS

$$(C, \Gamma(C)) \xrightarrow{\quad e \quad} (C \cup \{e\}, \Gamma(C \cup \{e\}))$$

where $\Gamma(\sigma)$ is the set of **credits** of σ:

$$\Gamma(\sigma) \quad = \quad \{e_i \in \overline{\sigma} \mid \overline{\sigma_i} \not\vdash e_i \;\wedge\; \overline{\sigma} \not\Vdash e_i\}$$

$A: \;\; b \Vdash a$

$B: \;\; a \vdash b$

$$\{\emptyset, \emptyset\} \xrightarrow{a} \{\{a\}, \{a\}\} \xrightarrow{b} \{\{b, a\}, \emptyset\}$$

$$\{\emptyset, \emptyset\} \xrightarrow{b} \{\{b\}, \{b\}\} \xrightarrow{a} \{\{b, a\}, \{b\}\}$$

Event structures with circular causality

CES = ES + circular enabling relation $\Vdash$

Plays $\sigma = e_0\, e_1\, e_2 \cdots$ are traces of the LTS

$$(C, \Gamma(C)) \xrightarrow{\quad e \quad} (C \cup \{e\}, \Gamma(C \cup \{e\}))$$

where $\Gamma(\sigma)$ is the set of **credits** of σ:

$$\Gamma(\sigma) \;\; = \;\; \{e_i \in \overline{\sigma} \mid \overline{\sigma_i} \nvdash e_i \;\wedge\; \overline{\sigma} \nVdash e_i\}$$

$A :\;\; b \Vdash a$
$B :\;\; a \vdash b$

$$\{\emptyset, \emptyset\} \xrightarrow{a} \{\{a\}, \{a\}\} \xrightarrow{b} \{\{b, a\}, \emptyset\}$$

$$\{\emptyset, \emptyset\} \xrightarrow{b} \{\{b\}, \{b\}\} \xrightarrow{a} \{\{b, a\}, \{b\}\}$$

Prudent events (bloody definition)

A is **innocent** in $\sigma = e_0 \, e_1 \cdots$ iff:

$$\forall e \text{ of A}. \ \forall i \geq 0. \ \exists j \geq i. \ e \text{ not prudent in } \sigma_j$$

e is **prudent** in σ if $\exists \, \Sigma$ prudent strategy such that $e \in \Sigma(\sigma)$

Σ is a **prudent strategy** for A iff, for all fair plays σ' extending σ, conforming to Σ, and where all B $\neq$ A are innocent:

$$\exists k > |\sigma|. \ \Gamma(\sigma'_k) \cap \{\text{events of A}\} \subseteq \Gamma(\sigma)$$

Prudent events (bloody definition)

A is **innocent** in $\sigma = e_0\, e_1 \cdots$ iff:

$$\forall e \text{ of A. } \forall i \geq 0. \ \exists j \geq i. \ e \text{ not prudent in } \sigma_j$$

e is **prudent** in σ if $\exists\, \Sigma$ prudent strategy such that $e \in \Sigma(\sigma)$

Σ is a **prudent strategy** for A iff, for all fair plays σ' extending σ, conforming to Σ, and where all B $\neq$ A are innocent:

$$\exists k > |\sigma|. \ \ \Gamma(\sigma'_k) \cap \{\text{events of A}\} \subseteq \Gamma(\sigma)$$

Prudent events (bloody definition)

A is **innocent** in $\sigma = e_0\, e_1 \cdots$ iff:

$$\forall e \text{ of A. } \forall i \geq 0.\ \exists j \geq i.\ e \text{ not prudent in } \sigma_j$$

e is **prudent** in σ if $\exists\ \Sigma$ prudent strategy such that $e \in \Sigma(\sigma)$

Σ is a **prudent strategy** for A iff, for all fair plays σ' extending σ, conforming to Σ, and where all B $\neq$ A are innocent:

$$\exists k > |\sigma|.\ \ \Gamma(\sigma'_k) \cap \{\text{events of A}\} \subseteq \Gamma(\sigma)$$

Agreement AND Protection

Theorem. For circular payoffs for participants $A_1 \dots A_n$, there always exist CES-contracts $\mathcal{C}_1 \dots \mathcal{C}_n$ such that:

$$\mathcal{C}_1 \mid \cdots \mid \mathcal{C}_n \text{ admits an agreement}$$

AND

$$\forall i \in 1..n : \mathcal{C}_i \text{ protects } \mathsf{A}_i$$

This justifies extending ES with $\Vdash$. What about PCL and $\twoheadrightarrow$?

Agreement AND Protection

Theorem. For circular payoffs for participants $A_1 \ldots A_n$, there always exist CES-contracts $\mathcal{C}_1 \ldots \mathcal{C}_n$ such that:

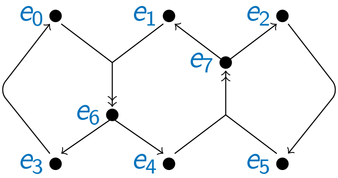
$$\mathcal{C}_1 \mid \cdots \mid \mathcal{C}_n \text{ admits an agreement}$$

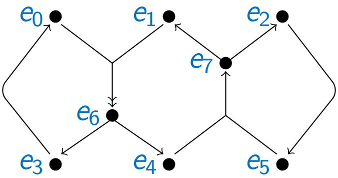
AND

$$\forall i \in 1..n : \mathcal{C}_i \text{ protects } \mathsf{A}_i$$

This justifies extending ES with $\Vdash$. What about PCL and $\twoheadrightarrow$?

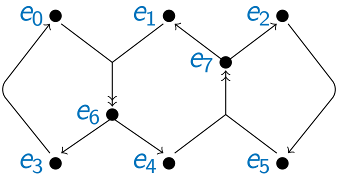
Quiz: which one admits an agreement?

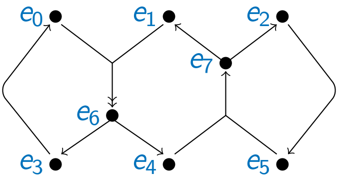




Provability in PCL is PSPACE-hard!

Quiz: which one admits an agreement?





Provability in PCL is PSPACE-hard!

Horn PCL $\sim$ conflict-free CES

Conflict-free CES are isomorphic to Horn PCL theories:

$$X \vdash e \quad \sim \quad (\bigwedge X) \to e$$
$$X \Vdash e \quad \sim \quad (\bigwedge X) \twoheadrightarrow e$$

Example.

- CES: $b \vdash a$, $a \Vdash b$ Reachable events: a, b
- PCL: $b \to a$, $a \twoheadrightarrow b$ Provable atoms: a, b

Th. If $\mathcal{E} \sim \Delta$, then

reachable events in $\mathcal{E}$ = provable atoms in Δ

A logical characterization of agreement

A reachability payoff is defined by a set of sets of events φ such that:

$$\sigma \in \Phi \iff \overline{\sigma} \in \varphi$$

(i.e., the order of events is immaterial)

Th. If $\mathcal{E} \sim \Delta$, and Φ is a reachability payoff (defined by φ):

- $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ admits an agreement $\iff \{a \mid \Delta \vdash a\} \in \varphi$
- there exists a PTIME algorithm for agreement

What relation between winning strategies and PCL?

A logical characterization of agreement

A reachability payoff is defined by a set of sets of events φ such that:

$$\sigma \in \Phi \iff \overline{\sigma} \in \varphi$$

(i.e., the order of events is immaterial)

Th. If $\mathcal{E} \sim \Delta$, and Φ is a reachability payoff (defined by φ):

- $\mathcal{C} = \langle \mathcal{E}, \Phi \rangle$ admits an agreement $\iff \{a \mid \Delta \vdash a\} \in \varphi$
- there exists a PTIME algorithm for agreement

What relation between winning strategies and PCL?

Proof traces

Proof in Horn PCL induce an ordering among atoms, e.g. in

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

atom a is proved after all the atoms in α have been proved.

Example:

$$\Delta_1 = \{a \to b,\ a\}$$
$$[\![\Delta_1]\!] = \{\varepsilon,\ a,\ ab\}$$

Note: $ba \notin [\![\Delta_1]\!]$

Example:

$$\Delta_2 = \{a \to b,\ b \to a\}$$
$$[\![\Delta_2]\!] = \{\varepsilon\}$$

Proof traces (2)

Elimination of $\alpha \twoheadrightarrow a$ does not require to prove α before a:

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

because a can be used as hypothesis.

Example:

$$\Delta_3 = \{a \twoheadrightarrow b,\ b \twoheadrightarrow a\}$$
$$[\![\Delta_3]\!] = \{\varepsilon,\ ab,\ ba\}$$

Note: $a, b \notin [\![\Delta_3]\!]$

Example:

$$\Delta_4 = \{a \rightarrow b,\ b \twoheadrightarrow a\}$$
$$[\![\Delta_4]\!] = \{\varepsilon,\ ab\}$$

Note: $a, b, ba \notin [\![\Delta_4]\!]$

Proof traces (3)

$$\frac{}{\varepsilon \in [\![\Delta]\!]}$$

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

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

Th. $\Delta \vdash a \iff \exists \sigma \in [\![\Delta]\!].\ a \in \overline{\sigma}$

(both concatenation and interleaving remove rightmost duplicates)

Prudent plays *vs.* Proof traces

Say a play $\sigma = e_0\, e_1 \cdots$ **prudent** when $\forall i :\ e_i$ is prudent in σ_i.

Th. If $\mathcal{C} = \langle \mathcal{E}, \cdots \rangle$ and $\mathcal{E} \sim \Delta$, then:

$$\sigma \text{ is a prudent play of } \mathcal{C} \iff \exists \eta.\ \sigma\, \eta \in [\![\Delta]\!]$$

Winning strategies via PCL

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

$$\Sigma_{\mathsf{A}}(\sigma) \;\; = \;\; \{a \text{ of } \mathsf{A} \mid \exists \sigma_1, \sigma_2.\;\; a \not\in \overline{\sigma} = \overline{\sigma_1} \;\wedge\; \sigma_1\, a\, \sigma_2 \in [\![\Delta, \overline{\sigma}]\!]\}$$

Then:

- Σ_{A} is a prudent strategy for A in $\mathcal{C} = \langle \mathcal{E}, \cdots \rangle$.
- If $\mathcal{C}$ admits an agreement (with a reachability payoff) then Σ_{A} is a winning strategy for A.

Thanks!