Extend Commitment Protocols with Temporal Regulations: Why and How

Elisa Marengo

Advisor: Matteo Baldoni

Co-advisor: Cristina Baroglio

Università degli Studi di Torino.

{emarengo, baldoni, baroglio}@di.unito.it

What I will talk about

We want to find a *coordination* mechanism for

- *autonomous agents*

in the context of

- *open*

- *heterogeneous*

systems

**Figure**: Coordination schema by M. Huns & L. Stephens [Weiss, 1999]

---

**Interaction protocols’ point of view**

do not make assumptions on the agents’ behaviour
What I will talk about

We want to find a **coordination** mechanism for

- **autonomous agents**

in the context of

- **open**

- **heterogeneous**

systems

**Figure:** Coordination schema by M. Huns & L. Stephens [Weiss, 1999]

**Interaction protocols’ point of view**

do not make assumptions on the agents’ behaviour
The context

To solve the coordination task we have to be aware that

- **protocols**: they need to be verifiable
- **autonomy**: no introspection
  - No mentalistic approaches for coordination
  - Only observable behaviour can be judged
- **autonomy**: we cannot tell agents what to do
  - No procedural approaches
  - No methods invocation: they are not objects
  - It is not planning
- **heterogeneity**: no assumptions on their implementation
  - They belongs to different owners
  - We know the roles, not the players
Commitment Protocols?

Commitment protocols [Singh, 2000, Yolum and Singh, 2001a]:

\[ C(\text{debtor}, \text{creditor}, \text{antecedent}, \text{consequent}) \]

- **Social state:** contains commitments and other literals that are relevant to their interaction;
- **Social actions:** defined in terms of operations onto the social state;
- **Regulative nature:** debtors should act in accordance with the commitments they have taken.

They meet the requirements

- do not impose actions to the agents (*respecting autonomy*)
- social and observational semantics of the communication
  - no introspection (*respecting autonomy and heterogeneity*)
  - they are verifiable (*according to protocol requirement*)
- coordination is realized by means of social expectations (*respecting autonomy and heterogeneity*)
Commitment Protocols?

Commitment protocols [Singh, 2000, Yolum and Singh, 2001a]:

$$C(\text{debtor}, \text{creditor}, \text{antecedent}, \text{consequent})$$

- **Social state**: contains commitments and other literals that are relevant to their interaction;
- **Social actions**: defined in terms of operations onto the social state;
- **Regulative nature**: debtors should act in accordance with the commitments they have taken.

They meet the requirements

- do not impose actions to the agents (*respecting autonomy*)
- social and observational semantics of the communication
  - no introspection (*respecting autonomy and heterogeneity*)
  - they are verifiable (*according to protocol requirement*)
- coordination is realized by means of *social expectations* (*respecting autonomy and heterogeneity*)
What is missing?

Commitment protocols

- realize coordination through **what** condition is to be achieved [Winikoff et al., 2005]
- disregard coordination through **how** conditions should be achieved: **temporal ordering** [Baldoni et al., 2010]

Temporal regulations

To rule the evolution of the social state distinguishing

- legal evolutions
- undesired evolutions

Temporal regulations define **patterns of interaction** that

- represent conventions, norms, preferences, habits, rules and suchlike
- allow for prevision: agents can have expectations on each others’ behaviour
How to specify patterns of interaction?

In a way that:

- does not compromise the flexibility of agents' behaviour
- does not compromise the agents' autonomy
- fosters openness (agents can easily enter/leave a system)
- introduces modularity:
  - easier re-use of protocols in different contexts
  - easier customization of protocols
  - easier composition of protocols
To meet these requirements

enhanced commitment-based protocol formal framework [Baldoni et al., 2011]:

- explicit distinction between a constitutive and a regulative specification [Searle, 1969] of the protocol
- **constitutive specification**: how actions affect the social state
- **regulative specification**: rules the evolution of the social state
Constitutive specification

\[ A \rightarrow (Action \textbf{means} Operation \textbf{if} Cond)^+ \]

\[ Action \rightarrow protocolAction \]

\[ Operation \rightarrow Op(commitment) \mid fact \mid Operation \wedge Operation \]

\[ Op \rightarrow CREATE \mid DELETE \mid RELEASE \mid DELEGATE \mid ASSIGN \mid \ldots \]

\[ Cond \rightarrow literal \mid Cond \wedge Cond \mid Cond \vee Cond \mid Cond \text{ XOR } Cond \]

- the \textit{means} construct amounts to a \textit{counts-as} relation [Searle, 1995]
- similar to [Chopra, 2009, Singh, 1999, Yolum and Singh, 2001b]
Regulative specification

<table>
<thead>
<tr>
<th>2CL: Constraints among Commitment Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>allows <em>declarative, constraint-based</em> representation of <em>patterns of interaction</em></td>
</tr>
<tr>
<td>• we defined a set of operators and their negations [Baldoni et al., 2010]</td>
</tr>
<tr>
<td>• grounded on LTL</td>
</tr>
<tr>
<td>• allows for the specification of constraints among literals and commitments</td>
</tr>
<tr>
<td>• constraints have a <em>regulative nature</em>:</td>
</tr>
<tr>
<td>▶ intuitively: restrict the set of legal execution paths</td>
</tr>
<tr>
<td>▶ <em>do not</em> specify <em>which</em> actions should bring conditions about</td>
</tr>
<tr>
<td>▶ <em>any</em> evolution, of the social state, that respects the constraints respects the protocol</td>
</tr>
<tr>
<td>Relation</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Correlation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Co-existence</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Response</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Before</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cause</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Premise</td>
</tr>
<tr>
<td>Immediate after</td>
</tr>
</tbody>
</table>

**Table:** 2CL constraint relations and their semantics in LTL.
A commitment machine for our protocols

Legal executions

- a legal execution of a commitment-based protocols enriched with 2CL regulative specification:
  - is accepted by the commitment machine built upon the constitutive specification [Winikoff et al., 2005]
  - satisfies the LTL formulas corresponding to the regulative specification

We implemented an extension of Winikoff et al.’s enhanced commitment machine [Winikoff et al., 2005]

- the output is an annotated and colored graph of the possible interactions
  - paths represent the possible interactions given the constitutive specification
  - annotations highlights violations and unsatisfied constraints

- by working on facts and events, and by considering a subset of LTL: verification can be performed on states, rather than on paths
Modularity for Business Protocols

In the context of regulations that change along time

- Business protocols must be compliant to regulations
- Modularity simplifies the task of adapting them to the new regulations

- New regulations usually impose the execution of new activities to be interleaved with the previous existing one
- Modularity is needed to simplify the grafting of the new regulations onto existing business protocols

By separating constitutive and regulative specification

- New activities are added to the constitutive specification of the protocols
- New temporal regulations declaratively specify when, how, where the added activities are to be used: grafting points
Modularity for Business Protocols

In the context of regulations that change along time

- business protocols must be *compliant to regulations*
- **modularity** simplifies the task of adapting them to the new regulations

- new regulations usually impose the execution of new activities to be interleaved with the previous existing one
- modularity is needed to simplify the **grafting** of the new regulations onto existing business protocols

By separating constitutive and regulative specification

- **new activities** are added to the constitutive specification of the protocols
- **new temporal regulation** declaratively specify *when, how, where* the added activities are to be used: **grafting points**
A Real-world Case Study: OECD Guidelines

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:

- protecting data owners from the violation of their fundamental rights
- encouraging the flow of data by increasing trust between countries

Pre-guidelines Data Flow Protocol

(a) \text{ask\_data means asked\_data if } \neg \text{asked\_data}.

(b) \text{send\_data means sent\_data if asked\_data } \land \neg \text{sent\_data } \land \neg \text{refuse\_data}.

(c) \text{refuse\_data means refuse\_data, CANCEL(C(dc, asker, sent\_data)) if asked\_data } \land \neg \text{sent\_data } \land \neg \text{refuse\_data}.
Grafting of OECD Guidelines

New activities

(d) \texttt{periodically\_verify\_accuracy} \textbf{means} \texttt{accuracy\_verified}
   \hspace{1cm} \textbf{if} \hspace{0.5cm} \neg \texttt{asked\_data} \hspace{0.5cm} \wedge \hspace{0.5cm} \neg \texttt{accuracy\_verified}.

(e) \texttt{check\_accuracy} \textbf{means} \texttt{accuracy\_verified}
   \hspace{1cm} \textbf{if} \hspace{0.5cm} \texttt{asked\_data} \hspace{0.5cm} \wedge \hspace{0.5cm} \neg \texttt{accuracy\_verified}.

(f) \texttt{verify\_purpose} \textbf{means} \texttt{purpose\_verified}
   \hspace{1cm} \textbf{if} \hspace{0.5cm} \texttt{asked\_data} \hspace{0.5cm} \wedge \hspace{0.5cm} \neg \texttt{purpose\_verified}.

(g) \texttt{notify\_owner} \textbf{means} \texttt{owner\_notified}
   \hspace{1cm} \textbf{if} \hspace{0.5cm} \texttt{sent\_data} \hspace{0.5cm} \wedge \hspace{0.5cm} \neg \texttt{owner\_notified}.

New regulations

(c1) \texttt{purpose\_verified} \rightarrow \bullet \texttt{sent\_data}
(c2) \texttt{accuracy\_verified} \rightarrow \bullet \texttt{sent\_data}
(c3) \texttt{sent\_data} \leftrightarrow \texttt{owner\_notified}
(c4) \texttt{purpose\_verified} \rightarrow \bullet \texttt{refuse\_data}
(c5) \texttt{accuracy\_verified} \rightarrow \bullet \texttt{refuse\_data}
**Figure:** Reachability graph for the Data Flow protocol extended with OECD Guidelines.
A tool for the analysis

This tool can be used by the analysts in order to:

- identify the risk of violations the interaction can encounter
- helping the decision on when to apply regimentation or enforcement
  [Jones and Sergot, 1994]
A Real-world Case Study: MiFID

- MiFID: Markets in Financial Instruments Directive
- protection of the clients of financial service agencies
- introduces new regulations that financial services must follow

Constitutive specification

(a) `propose_solution` means `proposed_RiskL` if ....
(b) `reject_proposal` means `rejected_proposal`, `RELEASE(C(fp, inv, invested))` if ...
(c) `sign_order` means `CREATE(C(inv, bank, contract Ended)), accepted_proposal, order_signed` if ...
(d) `countersign_contract` means `contract_countersigned, CREATE(C(bank, inv, executed_order)), invested` if ...
(e) `send_contract` means `contract_sent` if ...
(f) `notify` means `notified` if ...
(g) `end` means `executed_order, contract Ended` if ...

Regulative specification

(c1) `notified` $\rightarrow\Box contract_ended$
(c2) `contract_sent` $\rightarrow\Box notified$
MiFID regulation

- MiFID dictates how the interaction with the client should be carried
- violation of some constraint does not affect the sale directly, but creates a risk of sanction and a risk of exposure for the intermediary

**New activities**

(h) interview means investor_identified, document_supplied if . . .
(i) profile means CREATE(C(fp, inv, evaluation)), investor_classified if ¬investor_classified ∧ investor_identified ∧ ¬contract Ended ∧ ¬contract_abort ∧ ¬rejected_proposal ∧ ¬fi_discarded.
(j) classify means classified if . . .
(k) fi_evaluation means CREATE(C(fp, inv, proposed_RiskL)), evaluation if . . .
(l) fi_discard means fi_discarded, CANCEL(C(fp, inv, invested)), CANCEL(C(fp, inv, proposed_RiskL)) if . . .
(m) order_verification means order_verified, CREATE(C(bank, inv, executed_order)) if . . .
(n) withdraw means contract_abort, RELEASE(C(bank, inv, executed_order)), CANCEL(C(inv, bank, contract Ended)) if . . .

**New regulations**

(c3) C(fp, inv, invested) •→ investor_identified ∧ document_supplied
(c4) investor_classified → C(fp, inv, propose_RiskL)
(c5) evaluation ∧ ¬fi_discarded → proposed_RiskL
(c6) order_verified → contract_countersigned
Current and Future work

- operational semantics for our commitment machine
- how to:
  - reify regulations into business relationships?
  - bring normative force to the specification?

First step: **Regula**, committing to regulations
[Elisa Marengo et al., 2011]

\[ C(\text{debtor}, \text{creditor}, \text{ant}_1 \cdot \text{ant}_2 \ldots, \text{cons}_1 \cdot \text{cons}_2 \ldots) \]

- temporal regulations can be expressed inside commitments
- ‘.’ (before [Singh, 2003]) is a temporal operator on events: *both events must occur and in the specified order*
About **Regula**

**Control**

It is the problem to establish whether an agent can bring about an event or complex action so as to detach or discharge a given commitment

- innate control
- social control

**Safety**

A commitment is safe for its debtor when the coordination necessary to fulfill the regulation is *supported* by commitments by the other agents involved, i.e. when:

- the debtor *controls* the negation of the antecedent (avoiding the commitment become active)
- or, whenever the antecedent holds, the debtor *controls* the residuation of the consequent (there is a way to satisfy the commitment)
Acknowledgments

I would like to thank the reviewers for the helpful suggestions, the mentors, my advisor Prof. Matteo Baldoni, and co-advisor Prof. Cristina Baroglio and Dr. Vivana Patti.


