Towards Model-Checking Contracts

Cristian Prisacariu — cristi@ifi.uio.no
Gerardo Schneider — gerardo@ifi.uio.no

Precise Modeling and Analysis group (PMA),
University of Oslo

First Workshop on Formal Languages and Analysis of Contract-Oriented Software

9^{th} of October 2007, Oslo, Norway.

Outline

Aim and Motivation

Our work:

- Formalizing and model checking contracts
- a formal Action-Based Contract Language $\mathcal{CL}$ and
- a formal basis for actions found in contracts
  - An algebra for actions found in contracts which is complete w.r.t. the
  - interpretation as guarded rooted trees
- give a direct semantics to $\mathcal{CL}$ on normative structures (ongoing)

In this paper:

- a model checking attempt
  - based on $\mathcal{CL}$
  - and the semantics into $\mathcal{C}\mu$-calculus
  - using NuSMV (maybe an extension of it)

Aim and Motivation

Our work:

- Formalizing and model checking contracts
- a formal Action-Based Contract Language $\mathcal{CL}$ and
- a formal basis for actions found in contracts
    - An algebra for actions found in contracts which is complete w.r.t. the
    - interpretation as guarded rooted trees
- give a direct semantics to $\mathcal{CL}$ on normative structures (ongoing)

In this paper:

- a model checking attempt
    - based on $\mathcal{CL}$
    - and the semantics into $\mathcal{C}\mu$-calculus
    - using NuSMV (maybe an extension of it)

Aim and Motivation

why a formal specification language?

Definition

A contract is a document which engages several parties in a transaction and stipulates commitments (obligations, rights, prohibitions), as well as penalties in case of contract violations.

A formal language for contracts should:

- remove the ambiguities of the natural language.
- restrict the user to writing only permitted clauses thus eliminating many of the usual mistakes.
- be able to represent the complex clauses of contracts especially Obligations, Permissions and Prohibitions.
- be amenable to verification by model checking techniques.

Aim and Motivation

why a formal specification language?

Definition

A contract is a document which engages several parties in a transaction and stipulates commitments (obligations, rights, prohibitions), as well as penalties in case of contract violations.

A formal language for contracts should:

- remove the ambiguities of the natural language.
- restrict the user to writing only permitted clauses thus eliminating many of the usual mistakes.
- be able to represent the complex clauses of contracts especially Obligations, Permissions and Prohibitions.
- be amenable to verification by model checking techniques.

Outline

The Contract Specification Language $\mathcal{CL}$

$$
\begin{array}{rcl}
\mathcal{C}ontract & := & \mathcal{D} \; ; \; \mathcal{C} \\
\mathcal{C} & := & \phi \mid \mathcal{C}_O \mid \mathcal{C}_P \mid \mathcal{C}_F \mid \mathcal{C} \wedge \mathcal{C} \mid [\alpha]\mathcal{C} \mid \langle\alpha\rangle\mathcal{C} \mid \mathcal{C}\,\mathcal{U}\,\mathcal{C} \mid \bigcirc\,\mathcal{C} \mid \Box\mathcal{C} \\
\mathcal{C}_O & := & O(\alpha) \mid \mathcal{C}_O \oplus \mathcal{C}_O \\
\mathcal{C}_P & := & P(\alpha) \mid \mathcal{C}_P \oplus \mathcal{C}_P \\
\mathcal{C}_F & := & F(\alpha) \mid \mathcal{C}_F \vee [\alpha]\mathcal{C}_F
\end{array}
$$

- ϕ denotes assertions and ranges over Boolean expressions including arithmetic comparisons, like “the budget is more than 200$”.
- $O(\alpha)$, $P(\alpha)$, $F(\alpha)$ specify obligation, permission (rights), and prohibition (forbidden) over actions
- α are complex actions constructed according to $\mathcal{CA}$ action algebra.
- $[\alpha]$ and $\langle\alpha\rangle$ are the action parameterized modalities of dynamic logic
- $\mathcal{U}$, $\bigcirc$, and $\Box$ are classical temporal logic operators
- $\wedge$, $\vee$, and $\oplus$ are conjunction, disjunction, and exclusive disjunction

The Contract Specification Language $\mathcal{CL}$

$$
\begin{array}{rcl}
\mathcal{C}ontract & := & \mathcal{D} ; \mathcal{C} \\
\mathcal{C} & := & \phi \mid \mathcal{C}_O \mid \mathcal{C}_P \mid \mathcal{C}_F \mid \mathcal{C} \wedge \mathcal{C} \mid [\alpha]\mathcal{C} \mid \langle\alpha\rangle\mathcal{C} \mid \mathcal{C}\,\mathcal{U}\,\mathcal{C} \mid \bigcirc \mathcal{C} \mid \Box\mathcal{C} \\
\mathcal{C}_O & := & O(\alpha) \mid \mathcal{C}_O \oplus \mathcal{C}_O \\
\mathcal{C}_P & := & P(\alpha) \mid \mathcal{C}_P \oplus \mathcal{C}_P \\
\mathcal{C}_F & := & F(\alpha) \mid \mathcal{C}_F \vee [\alpha]\mathcal{C}_F
\end{array}
$$

- ϕ denotes assertions and ranges over Boolean expressions including arithmetic comparisons, like "the budget is more than 200$".
- $O(\alpha)$, $P(\alpha)$, $F(\alpha)$ specify obligation, permission (rights), and prohibition (forbidden) over actions
- α are complex actions constructed according to $\mathcal{CA}$ action algebra.
- $[\alpha]$ and $\langle\alpha\rangle$ are the action parameterized modalities of dynamic logic
- $\mathcal{U}$, $\bigcirc$, and $\Box$ are classical temporal logic operators
- $\wedge$, $\vee$, and $\oplus$ are conjunction, disjunction, and exclusive disjunction

Outline

Actions

- Actions are denoted by α and are constructed using the operators:
  - $+$ choice (idempotent)
  - $\cdot$ concatenation (sequencing)
  - & concurrent execution (not idempotent)
  - basic actions $\mathcal{A}_B$ and $\mathbf{0}$, $\mathbf{1}$.

$$\mathcal{CA} = (\mathcal{A}, +, \cdot, \&, \mathbf{0}, \mathbf{1})$$

  - $(\mathcal{A}, +, \cdot, \mathbf{0}, \mathbf{1})$ is an idempotent semiring
  - $(\mathcal{A}, +, \&, \mathbf{0}, \mathbf{1})$ is a idempotent and commutative semiring
  - & shuffles the sequences

    i.e. an *ordered* shuffle operator

    e.g. $(a \cdot b)\&(c \cdot d \cdot e) \;=\; a\&c \cdot b\&d \cdot e$

Concurrent actions

- constructed with the & operator: e.g. $d\&n$
- $O(d\&n) = O(d) \wedge O(n)$
- conflicting actions (cannot be done at the same time) like: "*go west*" and "*go east*"; then $O(w) \wedge O(e)$ is a conflicting clause.
- conflict relation : $a \#_{\mathcal{C}} b \stackrel{def}{\Longleftrightarrow} a\&b = \mathbf{0}$
- compatibility relation : $a \sim_{\mathcal{C}} b \stackrel{def}{\Longleftrightarrow} a\&b \neq \mathbf{0}$, where $a, b \neq \mathbf{0}$

- "*Whenever the Internet traffic is high (ϕ) then the client should pay (p) double immediately, or the client should notify (n) the service provider by sending an e-mail specifying that he delays (d) the payment.*"

  $\Box(\phi \implies O(p\&p) \oplus O(d\&n))$

More on the Contract Language

- Expressing contrary-to-duty (CTDs)
  $O_{\mathcal{C}}(\alpha) = O(\alpha) \wedge [\overline{\alpha}]\mathcal{C}$
- Expressing contrary-to-prohibition (CTPs)
  $F_{\mathcal{C}}(\alpha) = F(\alpha) \wedge [\alpha]\mathcal{C}$
- "In case the client delays the payment, after notification he must immediately lower the Internet traffic to the *low* level, and pay later twice. If the client does not lower the Internet traffic immediately, then the client will have to pay three times."
  $\Box([d\&n](O_{\mathcal{C}}(l) \wedge [l]\Diamond(O(p\&p))$ where $\mathcal{C} = \Diamond O(p\&p\&p)$
- There is a taste of resource-awareness in the actions.
  - Actions like $p\&p$ model discrete values.
  - Even though we have a finite set of atomic actions we get an infinite domain of the compound actions.
  - In work in progress we solve this infiniteness by using so-called *action schemas* (not in this paper)

Outline

$\mathcal{C}\mu$ – A variant of the modal μ-calculus

as the underlying logic

- The syntax of the $\mathcal{C}\mu$ logic
  $\varphi \;:=\; P \mid Z \mid P_c \mid \top \mid \neg\varphi \mid \varphi \wedge \varphi \mid [\gamma]\varphi \mid \mu Z.\varphi(Z)$

Four main differences with respect to the classical μ-calculus:

1. multisets of basic actions as labels: i.e. $\gamma = \{a, a, b\}$ is a label
   $m_\gamma : \mathcal{L} \rightarrow \mathbb{N}$, where $\mathcal{L}$ is the set of basic labels (representing actions)
   e.g.: $m_\gamma(a) = 2$ and $m_\gamma(b) = 1$
2. a set of propositional constants O_a and $\mathcal{F}_a$ one *for each basic action a*
3. a restriction to ensure that there cannot be at the same time an obligation and a prohibition of the same action:
   $||\mathcal{F}_a||^{\mathcal{T}}_{\mathcal{V}} \cap ||O_a||^{\mathcal{T}}_{\mathcal{V}} = \emptyset, \quad \forall a \in \mathcal{L}$
4. a restricted kind of determinism:
   from each state there are no two outgoing arrows labeled with the same action.

$\mathcal{C}\mu$ – A variant of the modal μ-calculus

semantics for the contract language

- semantics for the obligation
  $f^{\mathcal{T}}(O(\&_{i=1}^{n} a_i)) = \langle\{a_1, \ldots, a_n\}\rangle(\wedge_{i=1}^{n} O_{a_i})$
  e.g.: $f^{\mathcal{T}}(O(a\&b)) = \langle\{a, b\}\rangle(O_a \wedge O_b)$
  "The Provider is obliged to provide internet and telephony services (at the same time)"
- semantics for the prohibition
  $f^{\mathcal{T}}(F(\&_{i=1}^{n} a_i)) = [\{a_1, \ldots, a_n\}](\wedge_{i=1}^{n} \mathcal{F}_{a_i})$
  e.g.: $f^{\mathcal{T}}(F(a)) = [\{a\}](\mathcal{F}_a)$ often written as just $[a]\mathcal{F}_a$
  "Every action specified in the definition part which is not permitted at one moment is considered forbidden."
- semantics for the permission
  $f^{\mathcal{T}}(P(\&_{i=1}^{n} a_i)) = \langle\{a_1, \ldots, a_n\}\rangle(\wedge_{i=1}^{n} \neg\mathcal{F}_{a_i})$
  e.g.: $f^{\mathcal{T}}(P(a)) = \langle a\rangle\neg\mathcal{F}_a$

Translation function

$$
\begin{array}{llcl}
(1) & f^{\mathcal{T}}(O(\&_{i=1}^{n} a_i)) & = & \langle\{a_1, \ldots, a_n\}\rangle(\wedge_{i=1}^{n} O_{a_i}) \\
(2) & f^{\mathcal{T}}(\mathcal{C}_O \oplus \mathcal{C}_O) & = & f^{\mathcal{T}}(\mathcal{C}_O) \wedge f^{\mathcal{T}}(\mathcal{C}_O) \\
(3) & f^{\mathcal{T}}(P(\&_{i=1}^{n} a_i)) & = & \langle\{a_1, \ldots, a_n\}\rangle(\wedge_{i=1}^{n} \neg\mathcal{F}_{a_i}) \\
(4) & f^{\mathcal{T}}(\mathcal{C}_P \oplus \mathcal{C}_P) & = & f^{\mathcal{T}}(\mathcal{C}_P) \wedge f^{\mathcal{T}}(\mathcal{C}_P) \\
(5) & f^{\mathcal{T}}(F(\&_{i=1}^{n} a_i)) & = & [\{a_1, \ldots, a_n\}](\wedge_{i=1}^{n} \mathcal{F}_{a_i}) \\
(6) & f^{\mathcal{T}}(F(\delta) \vee [\beta]F(\delta)) & = & f^{\mathcal{T}}(F(\delta)) \vee f^{\mathcal{T}}([\beta]F(\delta)) \\
(7) & f^{\mathcal{T}}(\mathcal{C}_1 \wedge \mathcal{C}_2) & = & f^{\mathcal{T}}(\mathcal{C}_1) \wedge f^{\mathcal{T}}(\mathcal{C}_2) \\
(8) & f^{\mathcal{T}}(\bigcirc\mathcal{C}) & = & [\mathbf{any}]f^{\mathcal{T}}(\mathcal{C}) \\
(9) & f^{\mathcal{T}}(\mathcal{C}_1 \,\mathcal{U}\, \mathcal{C}_2) & = & \mu Z.f^{\mathcal{T}}(\mathcal{C}_2) \vee (f^{\mathcal{T}}(\mathcal{C}_1) \wedge [\mathbf{any}]Z \wedge \langle\mathbf{any}\rangle\top) \\
(10) & f^{\mathcal{T}}(\Box\mathcal{C}) & = & \nu Z.\mathcal{C} \wedge [\mathbf{any}]Z \\
(11) & f^{\mathcal{T}}([\&_{i=1}^{n} a_i]\mathcal{C}) & = & [\{a_1, \ldots, a_n\}]f^{\mathcal{T}}(\mathcal{C}) \\
(12) & f^{\mathcal{T}}([(\&_{i=1}^{n} a_i)\alpha]\mathcal{C}) & = & [\{a_1, \ldots, a_n\}]f^{\mathcal{T}}([\alpha]\mathcal{C}) \\
(13) & f^{\mathcal{T}}([\alpha + \beta]\mathcal{C}) & = & f^{\mathcal{T}}([\alpha]\mathcal{C}) \wedge f^{\mathcal{T}}([\beta]\mathcal{C}) \\
(14) & f^{\mathcal{T}}([\varphi?]\mathcal{C}) & = & f^{\mathcal{T}}(\varphi) \implies f^{\mathcal{T}}(\mathcal{C})
\end{array}
$$

DEMO

The contract example

1. The **Client** shall not:
a) supply false information to the Client Relations Department of the **Provider**.
2. Whenever the Internet Traffic is **high** then the **Client** must pay [*price*] immediately, or the **Client** must notify the **Provider** by sending an e-mail specifying that he will pay later.
3. If the **Client** delays the payment as stipulated in 2, after notification he must immediately lower the Internet traffic to the **normal** level, and pay later twice ($2 * [price]$).
4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 * [price]$.
5. The **Client** shall, as soon as the Internet Service becomes operative, submit within seven (7) days the Personal Data Form from his account on the **Provider**'s web page to the Client Relations Department of the **Provider**.
6. **Provider** may, at its sole discretion, without notice or giving any reason or incurring any liability for doing so:
a) Suspend Internet Services immediately if **Client** is in breach of Clause 1;

DEMO

Translating into $\mathcal{CL}$ syntax

1. $\Box F(fi)$

2. Whenever the Internet Traffic is **high** then the **Client** must pay [*price*] immediately, or the **Client** must notify the **Provider** by sending an e-mail specifying that he will pay later.
3. If the **Client** delays the payment as stipulated in 2, after notification he must immediately lower the Internet traffic to the **normal** level, and pay later twice ($2 * [price]$).
4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 * [price]$.
5. The **Client** shall, as soon as the Internet Service becomes operative, submit within seven (7) days the Personal Data Form from his account on the **Provider**'s web page to the Client Relations Department of the **Provider**.
6. **Provider** may, at its sole discretion, without notice or giving any reason or incurring any liability for doing so:
a) Suspend Internet Services immediately if **Client** is in breach of Clause 1;

DEMO

Translating into $\mathcal{CL}$ syntax

1. $\Box F_{P(s)}(fi)$

2. Whenever the Internet Traffic is **high** then the **Client** must pay [*price*] immediately, or the **Client** must notify the **Provider** by sending an e-mail specifying that he will pay later.
3. If the **Client** delays the payment as stipulated in 2, after notification he must immediately lower the Internet traffic to the **normal** level, and pay later twice $(2 * [price])$.
4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 * [price]$.
5. The **Client** shall, as soon as the Internet Service becomes operative, submit within seven (7) days the Personal Data Form from his account on the **Provider**'s web page to the Client Relations Department of the **Provider**.

DEMO

Translating into $\mathcal{CL}$ syntax

1. $\Box F_{P(s)}(fi)$

2. $\Box[h](\phi \implies O(p + (d \& n)))$

3. If the **Client** delays the payment as stipulated in 2, after notification he must immediately lower the Internet traffic to the **normal** level, and pay later twice $(2 * [price])$.
4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 * [price]$.
5. The **Client** shall, as soon as the Internet Service becomes operative, submit within seven (7) days the Personal Data Form from his account on the **Provider**'s web page to the Client Relations Department of the **Provider**.

DEMO

Translating into $\mathcal{CL}$ syntax

1. $\Box F_{P(s)}(fi)$

2. $\Box[h](\phi \implies O(p + (d\&n)))$

3. $\Box([d\&n](O(l) \wedge [l]\Diamond O(p\&p)))$

4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 * [price]$.
5. The **Client** shall, as soon as the Internet Service becomes operative, submit within seven (7) days the Personal Data Form from his account on the **Provider**'s web page to the Client Relations Department of the **Provider**.

DEMO

Translating into $\mathcal{CL}$ syntax

1. $\Box F_{P(s)}(fi)$

2. $\Box [h](\phi \implies O(p + (d\&n)))$

3. $\Box ([d\&n](O(l) \wedge [l]\Diamond O(p\&p)))$

4. $\Box ([d\&n \cdot \bar{l}\,]\Diamond O(p\&p\&p))$

5. The **Client** shall, as soon as the Internet Service becomes operative, submit within seven (7) days the Personal Data Form from his account on the **Provider**'s web page to the Client Relations Department of the **Provider**.

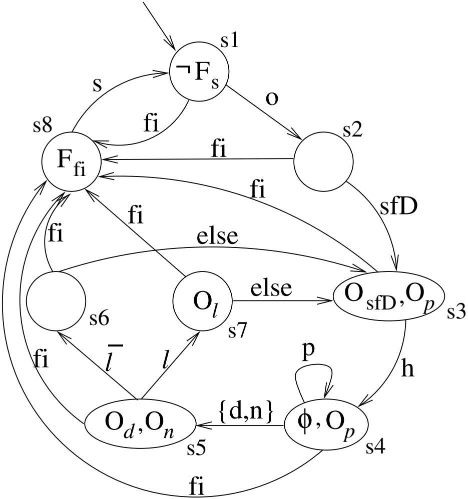
DEMO

Translating into $\mathcal{CL}$ syntax

1. $\Box F_{P(s)}(fi)$
2. $\Box[h](\phi \implies O(p + (d\&n)))$
3. $\Box([d\&n](O(l) \wedge [l]\Diamond O(p\&p)))$
4. $\Box([d\&n \cdot \bar{l}\,]\Diamond O(p\&p\&p))$
5. $\Box([o]O(sfD))$

DEMO

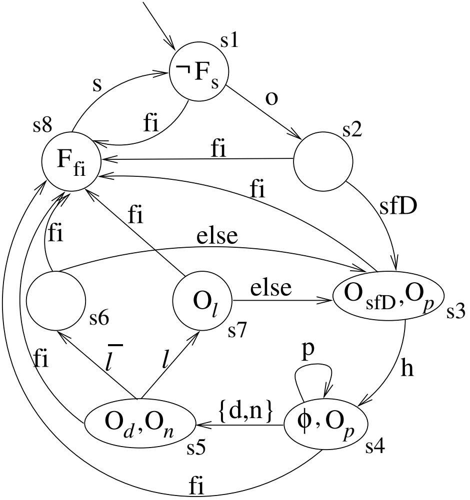
Handcrafting the model



DEMO

Handcrafting the model

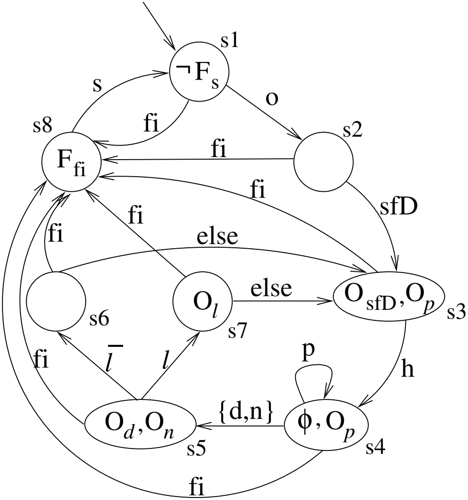
ϕ = the Internet traffic is high
fi = client supplies false information to Client Relations Department
h = client increases Internet traffic to *high* level
p = client pays [price]
d = client delays payment
n = client notifies by e-mail
l = client lowers the Int. traffic
sfD = client sends the Personal Data Form to Client Relations Department
o = provider activates the Internet Service (it becomes operative)
s = provider suspends service



DEMO

Testing the contract on the model: is OK!

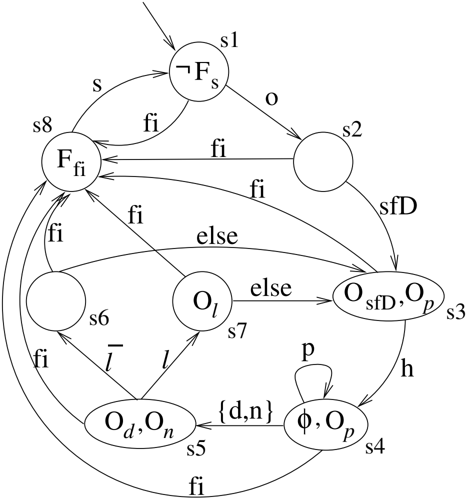
1. $\Box F_{P(s)}(fi)$
2. $\Box[h](\phi \implies O(p+(d\&n)))$
3. $\Box([d\&n](O(l) \wedge [l]\Diamond O(p\&p)))$
4. $\Box([d\&n \cdot \bar{l}\,]\Diamond O(p\&p\&p))$
5. $\Box([o]O(sfD))$



DEMO

Testing a property for the Client.

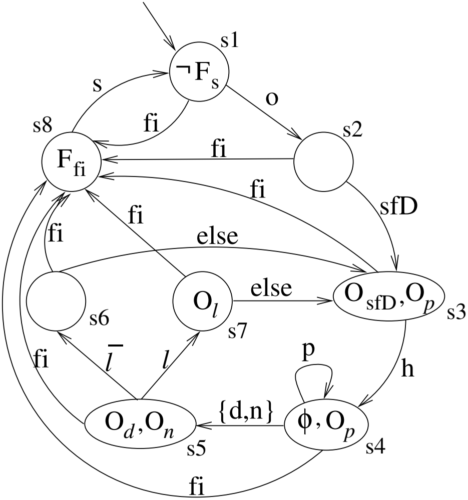
- "Is it the case that after the internet is high and the client pays then the client is obliged to pay again?"
- $\phi \wedge \langle p \rangle O(p)$
- "Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again"
- $\Box(\neg\phi \vee [p][p]\neg O_p)$
- "The provider guarantees that if the Internet traffic of the Client reaches a high level and the Client pays the [price] then it will not be obliged to pay the [price] again"



DEMO

Testing a property for the Client.

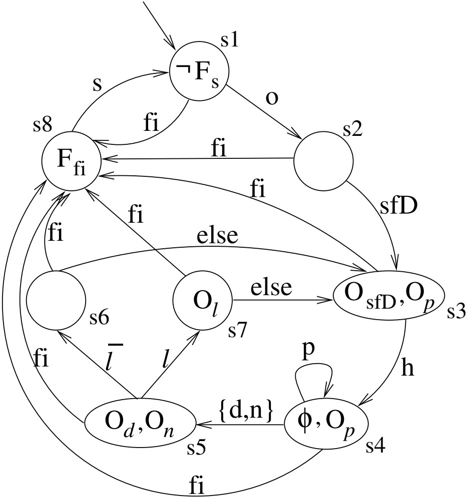
- "Is it the case that after the internet is high and the client pays then the client is obliged to pay again?"
- $\phi \wedge \langle p \rangle O(p)$
- "Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again"
- $\square(\neg\phi \vee [p][p]\neg O_p)$
- "The provider guarantees that if the Internet traffic of the Client reaches a high level and the Client pays the [price] then it will not be obliged to pay the [price] again"



DEMO

Testing a property for the Client.

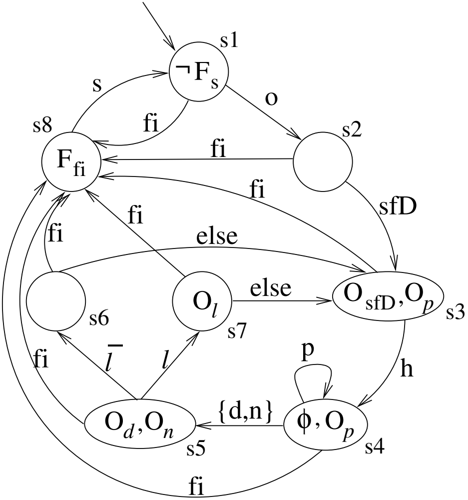
- "Is it the case that after the internet is high and the client pays then the client is obliged to pay again?"
- $\phi \wedge \langle p \rangle O(p)$
- "Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again"
- $\Box(\neg\phi \vee [p][p]\neg O_p)$
- "The provider guarantees that if the Internet traffic of the Client reaches a high level and the Client pays the [price] then it will not be obliged to pay the [price] again"



DEMO

Testing a property for the Client.

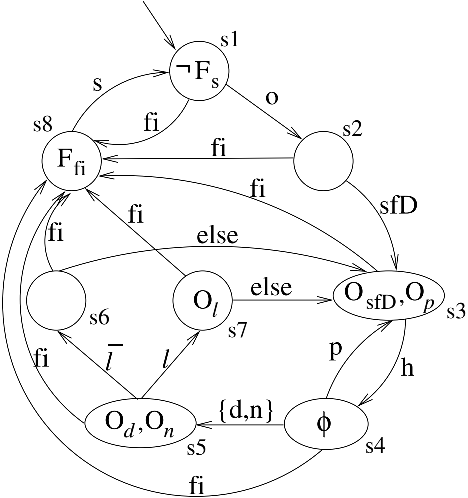
- "Is it the case that after the internet is high and the client pays then the client is obliged to pay again?"
- $\phi \wedge \langle p \rangle O(p)$
- "Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again"
- $\Box(\neg\phi \vee [p][p]\neg O_p)$
- "The provider guarantees that if the Internet traffic of the Client reaches a high level and the Client pays the [price] then it will not be obliged to pay the [price] again"



DEMO

Testing a property for the Client.

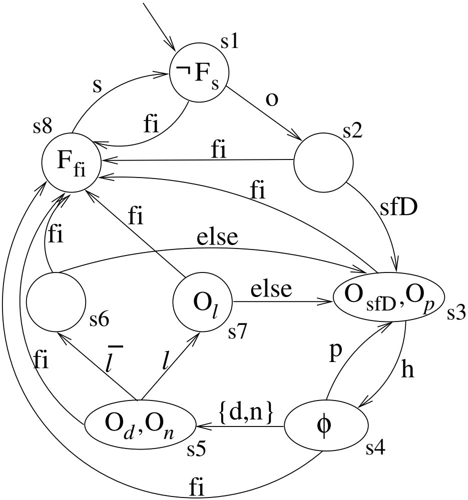
- "Is it the case that after the internet is high and the client pays then the client is obliged to pay again?"
- $\phi \wedge \langle p \rangle O(p)$
- "Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again"
- $\Box(\neg\phi \vee [p][p]\neg O_p)$
- "The provider guarantees that if the Internet traffic of the Client reaches a high level and the Client pays the [price] then it will not be obliged to pay the [price] again"



DEMO

Testing a property for the Supplier.

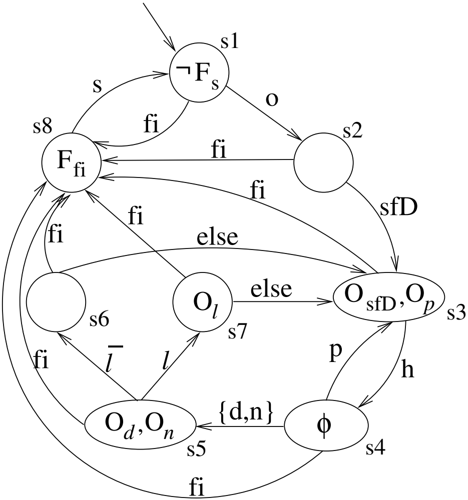
- "If the Internet is high and the client delays and notifies, and afterward lowers the Internet traffic, can it happen that the client does not pay twice until the internet traffic is high again?"
- $\Box(\phi \wedge [d\&n][l]\neg(\langle\overline{p\&p}\rangle\top\mathcal{U}\phi))$.
- $\Box([d\&n](O(l) \wedge [l](\neg\phi\mathcal{U}\, O(p\&p))))$.
- "after getting a high Internet traffic, if the client postpones the payment then the client can get a high traffic again only after having paid"



DEMO

Testing a property for the Supplier.

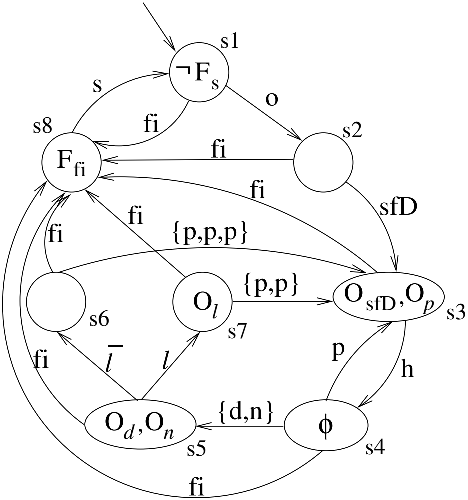
- "If the Internet is high and the client delays and notifies, and afterward lowers the Internet traffic, can it happen that the client does not pay twice until the internet traffic is high again?"
- $\Box(\phi \wedge [d\&n][l]\neg(\langle\overline{p\&p}\rangle\top\mathcal{U}\phi))$.
- $\Box([d\&n](O(l) \wedge [l](\neg\phi\mathcal{U}\, O(p\&p))))$.
- "after getting a high Internet traffic, if the client postpones the payment then the client can get a high traffic again only after having paid"



DEMO

Testing a property for the Supplier.

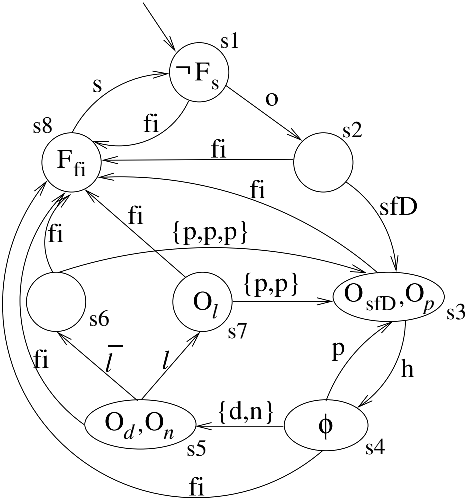
- "If the Internet is high and the client delays and notifies, and afterward lowers the Internet traffic, can it happen that the client does not pay twice until the internet traffic is high again?"
- $\Box(\phi \wedge [d\&n][l]\neg(\langle\overline{p\&p}\rangle\top\mathcal{U}\phi))$.
- $\Box([d\&n](O(l) \wedge [l](\neg\phi\mathcal{U}\, O(p\&p))))$.
- "after getting a high Internet traffic, if the client postpones the payment then the client can get a high traffic again only after having paid"



DEMO

Testing a property for the Supplier.

- "If the Internet is high and the client delays and notifies, and afterward lowers the Internet traffic, can it happen that the client does not pay twice until the internet traffic is high again?"
- $\Box(\phi \wedge [d\&n][l]\neg(\langle\overline{p\&p}\rangle\top\,\mathcal{U}\,\phi))$.
- $\Box([d\&n](O(l) \wedge [l](\neg\phi\,\mathcal{U}\,O(p\&p))))$.
- "after getting a high Internet traffic, if the client postpones the payment then the client can get a high traffic again only after having paid"



Conclusion

We have seen:

- A formal specification language based on actions for contracts with semantics in a variant of μ-calculus.
- The language is specially tailored for specifying contracts and adopts the view of obligations over actions
- An action algebra complete w.r.t. the interpretation of actions as guarded rooted trees
- A model checking methodology based on $\mathcal{CL}$ for contracts
- Play with NuSMV
- drawbacks

Further Work

- More model checking of case studies.
- Further theoretical investigations of the underlying actions and the semantics of the contract language.
- Model checking using the direct semantics; an extension for the NuSMV in this direction.
- The visual interpretation of the $\mathcal{CL}$ as normative diagrams.

Related Work

A. Daskalopulu '00 – contracts and Petri nets models

C. Molina-Jimenez et al. '03 – contracts and FSMs and SPIN

C. Pecheur & F. Raimondi '06 – NuSMV with actions

R. deNicola & F. Vaandragen '90 – Kripke structure $\longleftrightarrow$ LTS

K. Rozier & M.Y. Vardi '07 – LTL model generation survey

(Attempto) Controlled English (Natural Languages)

- `http://www.jfsowa.com/logic/ace.htm` (P. Sowa)
- `http://attempto.ifi.unizh.ch` (N. Fuchs)

COSoDIS home page `http://www.ifi.uio.no/cosodis/`

Thank you!

Related Work

A. Daskalopulu ’00 – contracts and Petri nets models

C. Molina-Jimenez et al. ’03 – contracts and FSMs and SPIN

C. Pecheur & F. Raimondi ’06 – NuSMV with actions

R. deNicola & F. Vaandragen ’90 – Kripke structure $\longleftrightarrow$ LTS

K. Rozier & M.Y. Vardi ’07 – LTL model generation survey

(Attempto) Controlled English (Natural Languages)

- `http://www.jfsowa.com/logic/ace.htm` (P. Sowa)
- `http://attempto.ifi.unizh.ch` (N. Fuchs)

COSoDIS home page `http://www.ifi.uio.no/cosodis/`

Thank you!