Towards Model-Checking Contracts

Cristian Prisacariu  Gerardo Schneider

cristi@ifi.uio.no  gerardo@ifi.uio.no

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

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

9th of October 2007, Oslo, Norway.
Outline

1. Aim and Motivation

2. The contract language $\mathcal{CL}$

3. Action Algebra

4. Mode Checking with NuSMV

5. Conclusion and Future Work
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 $C\mu$-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

1. Aim and Motivation
2. The contract language \( CL \)
3. Action Algebra
4. Mode Checking with NuSMV
5. Conclusion and Future Work
The Contract Specification Language $\mathcal{CL}$

\[\text{Contract} \quad := \quad D \; ; \; C\]
\[\mathcal{C} \quad := \quad \phi \; | \; \mathcal{C}_O \; | \; \mathcal{C}_P \; | \; \mathcal{C}_F \; | \; \mathcal{C} \; \land \; \mathcal{C} \; | \; [\alpha]C \; | \; \langle \alpha \rangle C \; | \; \mathcal{C} \; \cup \; \mathcal{C} \; | \; \bigcirc \; \mathcal{C} \; | \; \Box \; \mathcal{C}\]
\[\mathcal{C}_O \quad := \quad O(\alpha) \; | \; \mathcal{C}_O \; \oplus \; \mathcal{C}_O\]
\[\mathcal{C}_P \quad := \quad P(\alpha) \; | \; \mathcal{C}_P \; \oplus \; \mathcal{C}_P\]
\[\mathcal{C}_F \quad := \quad F(\alpha) \; | \; \mathcal{C}_F \; \lor \; [\alpha]C_F\]

- $\phi$ 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.
- $\alpha$ are complex actions constructed according to $\mathcal{CA}$ action algebra.
- $[\alpha]$ and $\langle \alpha \rangle$ are the action parameterized modalities of dynamic logic.
- $\land, \lor, \land$ are classical temporal logic operators.
- $\land, \lor, \land$ are conjunction, disjunction, and exclusive disjunction.
The Contract Specification Language $\mathcal{CL}$

$\text{Contract} := D ; C$

$C := \phi | C_O | C_P | C_F | C \land C | [\alpha]C | \langle \alpha \rangle C | C U C | \bigcirc C | \Box C$

$C_O := O(\alpha) | C_O \oplus C_O$

$C_P := P(\alpha) | C_P \oplus C_P$

$C_F := F(\alpha) | C_F \lor [\alpha]C_F$

- $\phi$ 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.
- $\alpha$ are complex actions constructed according to $\mathcal{CA}$ action algebra.
- $[\alpha]$ and $\langle \alpha \rangle$ are the action parameterized modalities of dynamic logic.
- $U, \bigcirc$, and $\Box$ are classical temporal logic operators.
- $\land, \lor$, and $\oplus$ are conjunction, disjunction, and exclusive disjunction.
Outline

1 Aim and Motivation

2 The contract language $CL$

3 Action Algebra

4 Mode Checking with NuSMV

5 Conclusion and Future Work
Actions

Actions are denoted by $\alpha$ and are constructed using the operators:

- $\cdot$ choice (idempotent)
- $\cdot$ concatenation (sequencing)
- $\cdot$ concurrent execution (not idempotent)
- basic actions $A_B$ and 0, 1.

$$CA = (A, +, \cdot, \&, 0, 1)$$

- $(A, +, \cdot, 0, 1)$ is an idempotent semiring
- $(A, +, \& , 0, 1)$ 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. \( d \& n \)
- \( O(d \& n) = O(d) \land O(n) \)
- conflicting actions (cannot be done at the same time) like: “go west” and “go east”; then \( O(w) \land O(e) \) is a conflicting clause.
- conflict relation: \( a \#_C b \iff a \& b = 0 \)
- compatibility relation: \( a \sim_C b \iff a \& b \neq 0 \), where \( a, b \neq 0 \)

“Whenever the Internet traffic is high (\( \phi \)) 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)
  \[ O_c(\alpha) = O(\alpha) \land [\alpha]C \]

- Expressing contrary-to-prohibition (CTPs)
  \[ F_c(\alpha) = F(\alpha) \land [\alpha]C \]

- “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.”
  \[ \Box([d\&n](O_c(l) \land [l]\Diamond(O(p&p))) \text{ where } C = \Diamond O(p&p&p)) \]

- 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

1. Aim and Motivation
2. The contract language $CL$
3. Action Algebra
4. Mode Checking with NuSMV
5. Conclusion and Future Work
\(C\mu\) – A variant of the modal \(\mu\)-calculus
as the underlying logic

- The syntax of the \(C\mu\) logic

\[ \varphi ::= P \mid Z \mid Pc \mid \top \mid \neg \varphi \mid \varphi \land \varphi \mid [\gamma] \varphi \mid \mu Z.\varphi(Z) \]

Four main differences with respect to the classical \(\mu\)-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 \(F_a\) 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:
   \(\|F_a\|^T_\gamma \cap \|O_a\|^T_\gamma = \emptyset\), \(\forall a \in \mathcal{L}\)

4. a restricted kind of determinism:
   from each state there are no two outgoing arrows labeled with the same action.
A variant of the modal $\mu$-calculus

semantics for the contract language

- semantics for the obligation
  \[ f^T (O(\&_{i=1}^n a_i)) = \langle \{a_1, \ldots, a_n\}\rangle (\wedge_{i=1}^n Oa_i) \]
e.g.: \[ f^T (O(a \& b)) = \langle \{a, b\}\rangle (Oa \land Ob) \]
  “The Provider is obliged to provide internet and telephony services (at the same time)”

- semantics for the prohibition
  \[ f^T (F(\&_{i=1}^n a_i)) = [\{a_1, \ldots, a_n\}](\wedge_{i=1}^n Fa_i) \]
e.g.: \[ f^T (F(a)) = [\{a\}](Fa) \] often written as just $[a]Fa$
  “Every action specified in the definition part which is not permitted at one moment is considered forbidden.”

- semantics for the permission
  \[ f^T (P(\&_{i=1}^n a_i)) = \langle \{a_1, \ldots, a_n\}\rangle (\wedge_{i=1}^n \neg Fa_i) \]
e.g.: \[ f^T (P(a)) = \langle a\rangle \neg Fa \]
Translation function

(1) \( f^T (O(\&_{i=1}^n a_i)) = \langle \{a_1, \ldots, a_n\} \rangle (\land_{i=1}^n O_{a_i}) \)
(2) \( f^T (C_O \oplus C_O) = f^T (C_O) \land f^T (C_O) \)
(3) \( f^T (P(\&_{i=1}^n a_i)) = \langle \{a_1, \ldots, a_n\} \rangle (\land_{i=1}^n \neg \mathcal{F}_{a_i}) \)
(4) \( f^T (C_P \oplus C_P) = f^T (C_P) \land f^T (C_P) \)
(5) \( f^T (F(\&_{i=1}^n a_i)) = [\{a_1, \ldots, a_n\}] (\land_{i=1}^n \mathcal{F}_{a_i}) \)
(6) \( f^T (F(\delta) \lor [\beta]F(\delta)) = f^T (F(\delta)) \lor f^T ([\beta]F(\delta)) \)
(7) \( f^T (C_1 \land C_2) = f^T (C_1) \land f^T (C_2) \)
(8) \( f^T (\Box C) = [\text{any}] f^T (C) \)
(9) \( f^T (C_1 \cup C_2) = \mu Z. f^T (C_2) \lor (f^T (C_1) \land [\text{any}] Z \land \langle \text{any} \rangle \top) \)
(10) \( f^T (\square C) = \nu Z. C \land [\text{any}] Z \)
(11) \( f^T ([\&_{i=1}^n a_i]C) = [\{a_1, \ldots, a_n\}] f^T (C) \)
(12) \( f^T ([\&(\&_{i=1}^n a_i)\alpha]C) = [\{a_1, \ldots, a_n\}] f^T ([\alpha]C) \)
(13) \( f^T ([\alpha + \beta]C) = f^T ([\alpha]C) \land f^T ([\beta]C) \)
(14) \( f^T ([\varphi?]C) = f^T (\varphi) \implies f^T (C) \)
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 $(2 \times [price])$.
4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 \times [price]$.
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. $\Box F(f_i)$

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 ($2 \times [price]$).

4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 \times [price]$.

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. $\Box F_{P(s)}(f_i)$

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. $\Box F_{P(s)}(f_i)$

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 ($2 \times [\text{price}]$).

4. If the Client does not lower the Internet traffic immediately, then the Client will have to pay $3 \times [\text{price}]$.

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.
Translating into $CL$ syntax

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

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

3. $\square ([d&n](O(l) \land [l] O(p&p)))$

4. If the **Client** does not lower the Internet traffic immediately, then the **Client** will have to pay $3 \times [price]$.

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. $\square F_{P(s)}(fi)$

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

3. $\square([d\&n](O(l) \land [l]\diamond O(p\&p)))$

4. $\square([d\&n \cdot \bar{I}]\diamond O(p\&p\&p))$

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

4. $\Box ([d&n \cdot \overline{I}]\Diamond O(p&p&p))$

5. $\Box ([o]O(sfD))$
DEMO
Handcrafting the model
\( \phi = \) the Internet traffic is high
\( f_i = \) 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. $\square F_{P(s)}(fi)$
2. $\square [h](\phi \implies O(p + (d\&n)))$
3. $\square ([d\&n](O(l) \land [l]\diamond O(p\&p)))$
4. $\square ([d\&n \cdot \bar{l}]\diamond O(p\&p\&p))$
5. $\square ([o]O(sfD))$
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?”
- $\phi \land \langle p \rangle O(p)$
- “Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again”
- $\Box(\neg \phi \lor [p][p] \neg O_p)$
- “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”
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?”

  $\phi \land \langle p \rangle O(p)$

- “Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again”

  $\square (\neg \phi \lor [p][p] \neg O_p)$

- “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”

$$\neg F_s$$
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?”
- \( \phi \land \langle p \rangle O(p) \)
- “Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again”
- \( \Box (\neg \phi \lor [p][p] \neg O_p) \)
- “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?”
  \[ \phi \land \langle p \rangle O(p) \]

- “Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again”
  \[ \Box (\neg \phi \lor [p][p]\neg O_p) \]

- “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”
  \[ F_{fi} \neg F_s \]

C. Prisacaru @ UiO
Towards Model-Checking Contracts
FLACOS 07 19 / 23
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?"
- $\phi \land \langle p \rangle O(p)$
- "Always it is not the case that after the internet is high and the client pays than the client is obliged to pay again"
- $\square(\neg \phi \lor [p][p] \neg O_p)$
- "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?”

¬Fs ∃[(φ ∧ [d&n]l) → (⟨p&p⟩U φ)].

□([d&n](O(l) ∧ [l](¬φ 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”
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?”

□(φ ∧ [d&n][l]¬((p&p) U φ)).

□([d&n](O(l) ∧ [l](¬φ 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?”

$$\Box (\phi \land [d \land n][l] \neg (\langle p \land p \rangle U \phi))$$.

$$\Box ([d \land n](O(l) \land [l](\neg \phi U O(p \land p))))$$.

“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”
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?”

\(\Box (\phi \land [d \& n][l] \neg (\langle p \& p \rangle \lor U \phi))\).

\(\Box ([d \& n](O(l) \land [l](\neg \phi U O(p \& p))))\).

“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 $\mu$-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 $CL$ 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 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 \(\leftrightarrow\) LTS
K. Rozier & M.Y. Vardi ’07 – LTL model generation survey

(Attempto) Controlled English (Natural Languages)
- [http://www.jfsowa.com/logic/ace.htm](http://www.jfsowa.com/logic/ace.htm) (P. Sowa)
- [http://attempto.ifi.unizh.ch](http://attempto.ifi.unizh.ch) (N. Fuchs)

COSoDIS home page [http://www.ifi.uio.no/cosodis/](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 $\leftrightarrow$ LTS
K. Rozier & M.Y. Vardi ’07 – LTL model generation survey

(Attempto) Controlled English (Natural Languages)

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

COSoDIS home page [http://www.ifi.uio.no/cosodis/](http://www.ifi.uio.no/cosodis/)

Thank you!