Compositional Specification of Commercial Contracts

Jesper Andersen, Ebbe Elsborg, Fritz Henglein,
Jakob Grue Simonsen, and Christian Stefansen
{jespera,elsborg,henglein,simonsen,cstef}@diku.dk

DIKU
Department of Computer Science
University of Copenhagen

A major French investment bank has costs of about 50 mio. Euro per year with about half due to legal costs in connection with contract disputes and the other half due to malexecution of financial contracts.

(Estimate by *Eber, 2002*)

Informal Contract Handling Must Be Replaced

Current informal contract handling is labor-intensive and problem-ridden.

The General Idea of Formal Contracts

Agreement to Sell Goods

Section 1. Seller shall sell and deliver to buyer (description of goods) no later than (date).

Section 2. In consideration hereof, buyer shall pay (amount in dollars) in cash on delivery.

The General Idea of Formal Contracts

Agreement to Sell Goods

Section 1. Seller shall sell and deliver to buyer (description of goods) no later than (date).

Section 2. In consideration hereof, buyer shall pay (amount in dollars) in cash on delivery.

```
sale (seller, buyer, goods, payment, t1, t2) =
     transmit (seller, buyer, goods, T | T < t1)
  || transmit (buyer, seller, payment, T | T < t2)
```

Contributions

We designed a declarative, compositional specification language for the basis of a contract life-cycle management system.

Contributions

We designed a declarative, compositional specification language for the basis of a contract life-cycle management system.

Let's consider contracts in the language in terms of:

1. Specification
2. Semantics
3. Execution
4. Analysis (future work!)

We Analyzed 15 Real-Life Contracts

How does one specify contracts?

To answer this we analyzed these commercial contracts:

Agreement to Sell Goods	Sale with Installment Payment
General Contract	Agreement to Sell
Balloon Note	Contractor Agreement
Legal Services Agreement	The Danish Trade Law
Website Development Contract	Lease Contract
Loan and Security Agreement	License Agreement
Operating Agreement	Supply Agreement
Manufacturing Agreement	

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Time

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Time

Events

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Time

Events

Structure:

Sequence

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Time

Events

Structure:

Sequence

Parallel

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Time

Events

Structure:

Sequence

Parallel

Choice

Agreement to Provide Legal Services

Section 1. The attorney shall provide, on a non-exclusive basis, legal services up to (n) hours per month, and furthermore provide services in excess of (n) hours upon agreement.

Section 2. In consideration hereof, the company shall pay a monthly fee of (amount in dollars) before the 8th day of the following month and (rate) per hour for any services in excess of (n) hours 40 days after the receival of an invoice.

Section 3. This contract is valid 1/1-12/31, 2004.

Data:

Agents

Resource

Time

Events

Structure:

Sequence

Parallel

Choice

Repetition

Syntax for Contract Specification

$\mathrm{Success}/\mathrm{Failure}$

The succeeded/failed contract with no commitments.

transmit$(A_1, A_2, R, T|P).c$

The commitment of agent A_1 to transmit resource R to agent A_2 at time T subject to predicate P (afterwards do contract c).

$c_1 ; c_1$

A sequence of two contracts. The first contract must be reduced to $\mathrm{Success}$ before the second can begin.

$c_1 \parallel c_2$

Parallel, independent execution of two contracts.

$c_1 + c_2$

(Non-deterministic) choice between two contracts.

$f(\vec{a})$

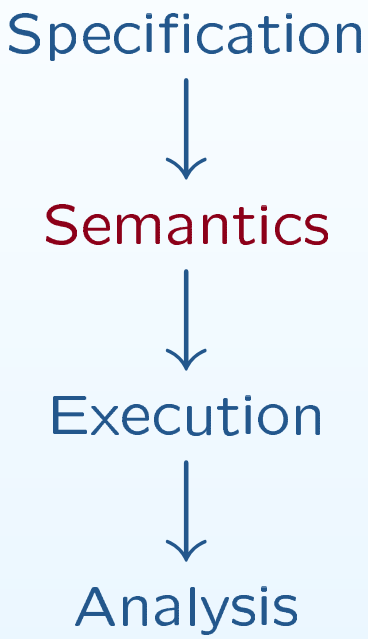
Expansion to body of contract f with arguments $\vec{a}$.

$\mathrm{letrec}\ f_i[\vec{X_i}] = c_i$ **in** c

Contract c with named contracts f_i with formal arguments X_i bound to c_i.

Legal Services Revisited

```
letrec
  legal (att, comp, hours, payment, extraprice, end, n) =
     transmit (att, comp, H, T | n <= T and T < n + 30 d and T <= end).
        (transmit (att, comp, invoice, T1 | hours < #(H, number, n + 30d)
          and #(invoice,total,T1) = (#(H,number,n) - hours) * extraprice).
         transmit(comp, att, #(invoice,total,T1), T2 | T2 <= T1+45)
         + Success)
     || (legal (att, comp, hours, payment, extraprice, end, n + 30 d)
          + Success)
  || transmit (comp, att, payment, T | T <= n + 40 d)
in
  legal ("Attorney", "Company", 20, 10000, 1200, 2004.12.31, 2004.1.1)
```


Specification
Semantics
Execution
Analysis

What Is the Meaning of a Contract?

Contracts denote sets of finite traces. A trace is a finite sequence of events:

$$s ::= \langle\rangle \mid \mathrm{transmit}(a_1, a_2, r, t)\ s$$

So contracts classify a given trace as performing or nonperforming. Formally, $\mathcal{C}[\![c]\!]^{\mathrm{D};\delta} = \{s : s \vdash^{\delta}_{\mathrm{D}} c\}$

The Satisfaction Relation

$$\frac{\delta \models P[a_1/A_1, a_2/A_2, r/R, t/T] \quad s \vdash^{\delta}_{\mathrm{D}} c[a_1/A_1, a_2/A_2, r/R, t/T]}{\mathrm{transmit}(a_1, a_2, r, t)\, s \vdash^{\delta}_{\mathrm{D}} \mathrm{transmit}((A_1, A_2, R, T|P)).\, c}$$

The Satisfaction Relation

$$\frac{\delta \models P[a_1/A_1, a_2/A_2, r/R, t/T] \quad s \vdash^{\delta}_{\mathrm{D}} c[a_1/A_1, a_2/A_2, r/R, t/T]}{\mathrm{transmit}(a_1, a_2, r, t)\, s \vdash^{\delta}_{\mathrm{D}} \mathrm{transmit}((A_1, A_2, R, T|P)).\, c}$$

$$\langle\rangle \vdash^{\delta}_{\mathrm{D}} \mathrm{Success}$$

The Satisfaction Relation

$$\frac{\delta \models P[a_1/A_1, a_2/A_2, r/R, t/T] \quad s \vdash^{\delta}_{\mathrm{D}} c[a_1/A_1, a_2/A_2, r/R, t/T]}{\mathrm{transmit}(a_1, a_2, r, t)\, s \vdash^{\delta}_{\mathrm{D}} \mathrm{transmit}((A_1, A_2, R, T|P)).\, c}$$

$$\langle\rangle \vdash^{\delta}_{\mathrm{D}} \mathrm{Success}$$

$$\frac{s_1 \vdash^{\delta}_{\mathrm{D}} c_1 \quad s_2 \vdash^{\delta}_{\mathrm{D}} c_2 \quad (s_1, s_2) \rightsquigarrow s}{s \vdash^{\delta}_{\mathrm{D}} c_1 \parallel c_2}$$

The Satisfaction Relation

$$\frac{\delta \models P[a_1/A_1, a_2/A_2, r/R, t/T] \quad s \vdash^{\delta}_{\mathrm{D}} c[a_1/A_1, a_2/A_2, r/R, t/T]}{\mathrm{transmit}(a_1, a_2, r, t)\, s \vdash^{\delta}_{\mathrm{D}} \mathrm{transmit}((A_1, A_2, R, T|P)).\, c}$$

$$\langle\rangle \vdash^{\delta}_{\mathrm{D}} \mathrm{Success}$$

$$\frac{s_1 \vdash^{\delta}_{\mathrm{D}} c_1 \quad s_2 \vdash^{\delta}_{\mathrm{D}} c_2 \quad (s_1, s_2) \rightsquigarrow s}{s \vdash^{\delta}_{\mathrm{D}} c_1 \parallel c_2}$$

What is $\mathcal{C}[\![\mathrm{Failure}]\!]^{\mathrm{D};\delta}$?

The Satisfaction Relation

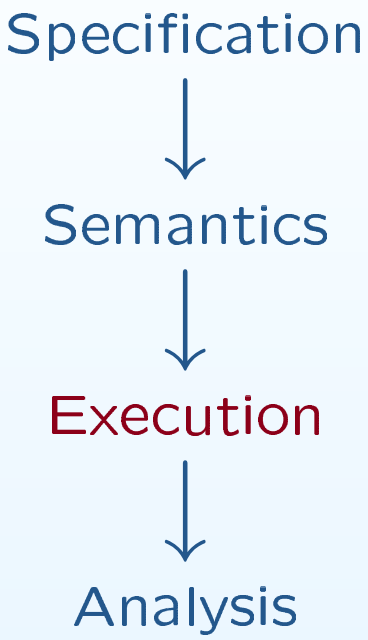
$$\frac{\delta \models P[a_1/A_1, a_2/A_2, r/R, t/T] \quad s \vdash^{\delta}_{\mathrm{D}} c[a_1/A_1, a_2/A_2, r/R, t/T]}{\mathrm{transmit}(a_1, a_2, r, t)\, s \vdash^{\delta}_{\mathrm{D}} \mathrm{transmit}((A_1, A_2, R, T|P)).\, c}$$

$$\langle\rangle \vdash^{\delta}_{\mathrm{D}} \mathrm{Success}$$

$$\frac{s_1 \vdash^{\delta}_{\mathrm{D}} c_1 \quad s_2 \vdash^{\delta}_{\mathrm{D}} c_2 \quad (s_1, s_2) \rightsquigarrow s}{s \vdash^{\delta}_{\mathrm{D}} c_1 \parallel c_2}$$

What is $\mathcal{C}[\![\mathrm{Failure}]\!]^{\mathrm{D};\delta}$?

The data model and the predicate language are orthogonal to the contract language. Plug in your own favorites!
To be general we just say $\mathrm{transmit}(\vec{X})$.


Specification
Semantics
Execution
Analysis

We Need a Represention of Residual Contracts

Define the *residuation function*:

$$S/e = \{s' \mid \exists s \in S : es' = s\}$$

We Need a Represention of Residual Contracts

Define the *residuation function*:

$$S/e = \{s' \mid \exists s \in S : es' = s\}$$

Let S_C denote the trace set of contract C. Trace sets are (most often) infinitely large – we need a better representation!

We Need a Represention of Residual Contracts

Define the *residuation function*:

$$S/e = \{s' \mid \exists s \in S : es' = s\}$$

Let S_C denote the trace set of contract C. Trace sets are (most often) infinitely large – we need a better representation!

It is not a priori clear whether S_C/e is denotable by a contract c'.

We Need a Represention of Residual Contracts

Define the *residuation function*:

$$S/e = \{s' \mid \exists s \in S : es' = s\}$$

Let S_C denote the trace set of contract C. Trace sets are (most often) infinitely large – we need a better representation!

It is not a priori clear whether S_C/e is denotable by a contract c'.

Luckily, this is the case if we impose one tiny contraint...

Only Consider Guarded Contracts

Consider the contract

$$f[\vec{X}] = (\text{transmit}(Y|P) + \text{Success}) \parallel f[\vec{X}].$$

Only Consider Guarded Contracts

Consider the contract

$$f[\vec{X}] = (\mathrm{transmit}(Y|P) + \mathrm{Success}) \parallel f[\vec{X}].$$

We introduce *guardedness*:

- To avoid the runtime system chasing around infinitely in this or arbitrarily complex other contracts that potentially denote the empty trace set.
- To thus make sure that every contract has a residual contract under any event.

Guarded Contracts

Intuitively, a contract is guarded if (mutual) recursions are prefixed by a transmit.

$$\mathrm{D} \vdash \text{Success guarded} \qquad \mathrm{D} \vdash \text{Failure guarded}$$

$$\mathrm{D} \vdash \text{transmit}(\vec{X} \mid P).\, c \text{ guarded} \qquad \frac{\mathrm{D} \vdash c \text{ guarded} \quad (f[\vec{X}] = c) \in \mathrm{D}}{\mathrm{D} \vdash f(\vec{a}) \text{ guarded}}$$

$$\frac{\mathrm{D} \vdash c \text{ guarded} \quad \mathrm{D} \vdash c' \text{ guarded}}{\mathrm{D} \vdash c + c' \text{ guarded}} \qquad \frac{\mathrm{D} \vdash c \text{ guarded} \quad \mathrm{D} \vdash c' \text{ guarded}}{\mathrm{D} \vdash c \parallel c' \text{ guarded}}$$

$$\frac{\mathrm{D} \not\models c \text{ nullable} \quad \mathrm{D} \vdash c \text{ guarded}}{\mathrm{D} \vdash c; c' \text{ guarded}}$$

$$\frac{\mathrm{D} \models c \text{ nullable} \quad \mathrm{D} \vdash c \text{ guarded} \quad \mathrm{D} \vdash c' \text{ guarded}}{\mathrm{D} \vdash c; c' \text{ guarded}}$$

Deterministic Reduction Thru Delayed Matching

Let's consider some rules from one of the possible reduction semantics:

$$\frac{\delta \models P[\vec{a}/\vec{X}]}{\mathrm{D}, \delta \vdash_D \mathrm{transmit}(\vec{X}|P).\, c \overset{\mathrm{transmit}(\vec{a})}{\longrightarrow} c[\vec{a}/\vec{X}]}$$

Deterministic Reduction Thru Delayed Matching

Let's consider some rules from one of the possible reduction semantics:

$$\frac{\delta \models P[\vec{a}/\vec{X}]}{\mathrm{D}, \delta \vdash_D \mathrm{transmit}(\vec{X}|P).\, c \overset{\mathrm{transmit}(\vec{a})}{\longrightarrow} c[\vec{a}/\vec{X}]}$$

$$\frac{\mathrm{D}, \delta \vdash_D c \overset{e}{\longrightarrow} d \quad \mathrm{D}, \delta \vdash_D c' \overset{e}{\longrightarrow} d'}{\mathrm{D}, \delta \vdash_D c + c' \overset{e}{\longrightarrow} d + d'}$$

Deterministic Reduction Thru Delayed Matching

Let's consider some rules from one of the possible reduction semantics:

$$\frac{\delta \models P[\vec{a}/\vec{X}]}{\mathrm{D}, \delta \vdash_D \mathrm{transmit}(\vec{X}|P).\, c \overset{\mathrm{transmit}(\vec{a})}{\longrightarrow} c[\vec{a}/\vec{X}]}$$

$$\frac{\mathrm{D}, \delta \vdash_D c \overset{e}{\longrightarrow} d \quad \mathrm{D}, \delta \vdash_D c' \overset{e}{\longrightarrow} d'}{\mathrm{D}, \delta \vdash_D c + c' \overset{e}{\longrightarrow} d + d'}$$

$$\frac{\mathrm{D}, \delta \vdash_D c \overset{e}{\longrightarrow} d \quad \mathrm{D}, \delta \vdash_D c' \overset{e}{\longrightarrow} d'}{\mathrm{D}, \delta \vdash_D c \parallel c' \overset{e}{\longrightarrow} c \parallel d' + d \parallel c'}$$

Guardedness Ensures Safe Residuation

Guarded Subject Reduction:

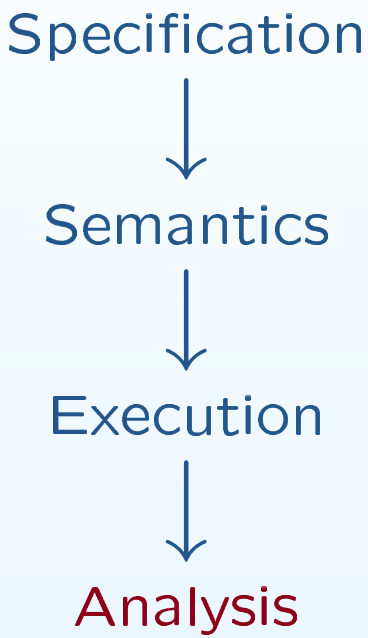
Theorem If $c \in \mathcal{C}^{\mathcal{P}}$ is guarded then for each event e there exists a unique $c' \in \mathcal{C}^{\mathcal{P}}$ such that $\mathrm{D}, \delta \vdash_D c \xrightarrow{e} c'$. Furthermore, we have that c' is guarded and $\mathrm{D}, \delta \models c/e = c'$, which means $\mathcal{C}[\![c]\!]^{\mathrm{D};\delta}/e = \mathcal{C}[\![c']\!]^{\mathrm{D};\delta}$. ◀

Guardedness Ensures Safe Residuation

Guarded Subject Reduction:

Theorem If $c \in \mathcal{C}^{\mathcal{P}}$ is guarded then for each event e there exists a unique $c' \in \mathcal{C}^{\mathcal{P}}$ such that $\mathrm{D}, \delta \vdash_D c \xrightarrow{e} c'$.
Furthermore, we have that c' is guarded and $\mathrm{D}, \delta \models c/e = c'$, which means $\mathcal{C}[\![c]\!]^{\mathrm{D};\delta}/e = \mathcal{C}[\![c']\!]^{\mathrm{D};\delta}$. ◀

Immediate payoff: Contracts can be used to represent trace sets. All functions on "original" contracts extend to residual contracts.


Specification
Semantics
Execution
Analysis

Contract Analysis Is Also Compositional

Future work!

Questions we would like to answer:

- What is my next order of business?
- What is this contract worth?
- What will this contract demand in terms of inventory/labor hours the next week/month?
- Is this contract consistent?

Contract Analysis Is Also Compositional

Future work!

Questions we would like to answer:

- What is my next order of business?
- What is this contract worth?
- What will this contract demand in terms of inventory/labor hours the next week/month?
- Is this contract consistent?

...enter financial engineering and stochastic programming!

Computing a Task List Is Easy!

Computing a Task List Is Easy!

$$\mathrm{D}, \delta, \mathrm{a}, t \vdash \mathrm{Success} \ : \ [] \qquad \mathrm{D}, \delta, \mathrm{a}, t \vdash \mathrm{Failure} \ : \ []$$

$$\frac{\models a \neq a_1 \qquad \vec{X} = (a_1, A, R, T)}{\mathrm{D}, \delta, \mathrm{a}, t \vdash \mathrm{transmit}(\vec{X} \mid [x; y]).\, c \ : \ \mathrm{do} \ []} \qquad \frac{\models t \notin [x; y]}{\mathrm{D}, \delta, \mathrm{a}, t \vdash \mathrm{transmit}(\vec{X} \mid [x; y]).\, c \ : \ \mathrm{do} \ [}$$

$$\frac{\models a = a_1 \qquad \vec{X} = (a_1, A, R, T) \qquad t \in [x; y]}{\mathrm{D}, \delta, \mathrm{a}, t \vdash \mathrm{transmit}(\vec{X} \mid [x; y]) \ : \ \mathrm{do} \ [\mathrm{transmit}(\vec{X} \mid [x; y])]}$$

$$\frac{\mathrm{D}, \delta, \mathrm{a}, t \vdash c_1 \ : \ l_1 \quad \mathrm{D}, \delta, \mathrm{a}, t \vdash c_2 \ : \ l_2}{\mathrm{D}, \delta, \mathrm{a}, t \vdash c_1 + c_2 \ : \ \mathrm{choose}[l_1, l_2]}$$

$$\frac{\mathrm{D} \vdash c_1 \ \mathrm{nullable} \qquad \mathrm{D}, \delta, \mathrm{a}, t \vdash c_1 \ : \ l_1 \qquad \mathrm{D}, \delta, \mathrm{a}, t \vdash c_2 \ : \ l_2}{\mathrm{D}, \delta, \mathrm{a}, t \vdash c_1; c_2 \ : \ \mathrm{choose}[l_1, l_2]}$$

$$\frac{\mathrm{D} \nvdash c_1 \ \mathrm{nullable} \qquad \mathrm{D}, \delta, \mathrm{a}, t \vdash c_1 \ : \ l_1}{\mathrm{D}, \delta, \mathrm{a}, t \vdash c_1; c_2 \ : \ l_1} \qquad \frac{\mathrm{D}, \delta, \mathrm{a}, t \vdash c_1 \ : \ l_1 \qquad \mathrm{D}, \delta, \mathrm{a}, t \vdash c_2 \ : \ l}{\mathrm{D}, \delta, \mathrm{a}, t \vdash c_1 \parallel c_2 \ : \ l_1 \ @ \ l_2}$$

Related Work

- Compositional Contracts (Peyton Jones, Eber, Seward, 2001)

Related Work

- Compositional Contracts (Peyton Jones, Eber, Seward, 2001)
- CSP (Communicating Sequential Processes) (C.A.R. Hoare, 1985)

Review

Specification – Semantics – Execution – Analysis

Review

Specification – Semantics – Execution – Analysis

- The compositional approach is viable!

Review

Specification – Semantics – Execution – Analysis

- The compositional approach is viable!
- Contract handling has been broken for a while now.

Review

Specification – Semantics – Execution – Analysis

- The compositional approach is viable!
- Contract handling has been broken for a while now.
- Huge sums are being wasted because of bad systems.

Review

Specification – Semantics – Execution – Analysis

- The compositional approach is viable!
- Contract handling has been broken for a while now.
- Huge sums are being wasted because of bad systems.
- Business systems will be the next heyday for theoretical computer science.

Review

Specification – Semantics – Execution – Analysis

- The compositional approach is viable!
- Contract handling has been broken for a while now.
- Huge sums are being wasted because of bad systems.
- Business systems will be the next heyday for theoretical computer science.

Thank you!

More Information

Read the technical report at:

`http://topps.diku.dk/next/contracts/`

Visit our homepage:

`http://www.it.edu/next`

Write an email:

`cstef@diku.dk`