A Rewriting Framework and Logic for Activities Subject to Regulations

Max Kanovich[1], Tajana Ban Kirigin[2], Vivek Nigam[3],
Andre Scedrov[4], Carolyn Talcott[5], Ranko Perović[6]

[1] Queen Mary, University of London, UK

[2] University of Rijeka, HR

3 Federal University of Paraíba, João Pessoa, Brazil

[4] University of Pennsylvania, USA

[5] SRI International, USA

[6] Clinical Research Manager, USA

A Rewriting Framework and Logic for Activities Subject to Regulations

M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. L. Talcott, R. Perović.

- Towards an automated assistant for clinical investigations.
  IHI, 2012.
- A rewriting framework for activities subject to regulations.
  RTA, 2012.
- A rewriting framework and logic for activities subject to regulations.
  MSCS, 2015.

Motivational Application: Clinical Investigations

Motivational Application: Clinical Investigations

- Before drugs can be made available to the general public, their effectiveness has to be experimentally validated.
- At the final stages tests that involve human subjects are carried out. These tests are called **Clinical Investigations**.

Motivational Application: Clinical Investigations

- Before drugs can be made available to the general public, their effectiveness has to be experimentally validated.
- At the final stages tests that involve human subjects are carried out. These tests are called **Clinical Investigations**.

Key Concerns

Safety of Subjects

One should avoid at all costs that the health of subjects is compromised during the tests.

Conclusive Data Collection

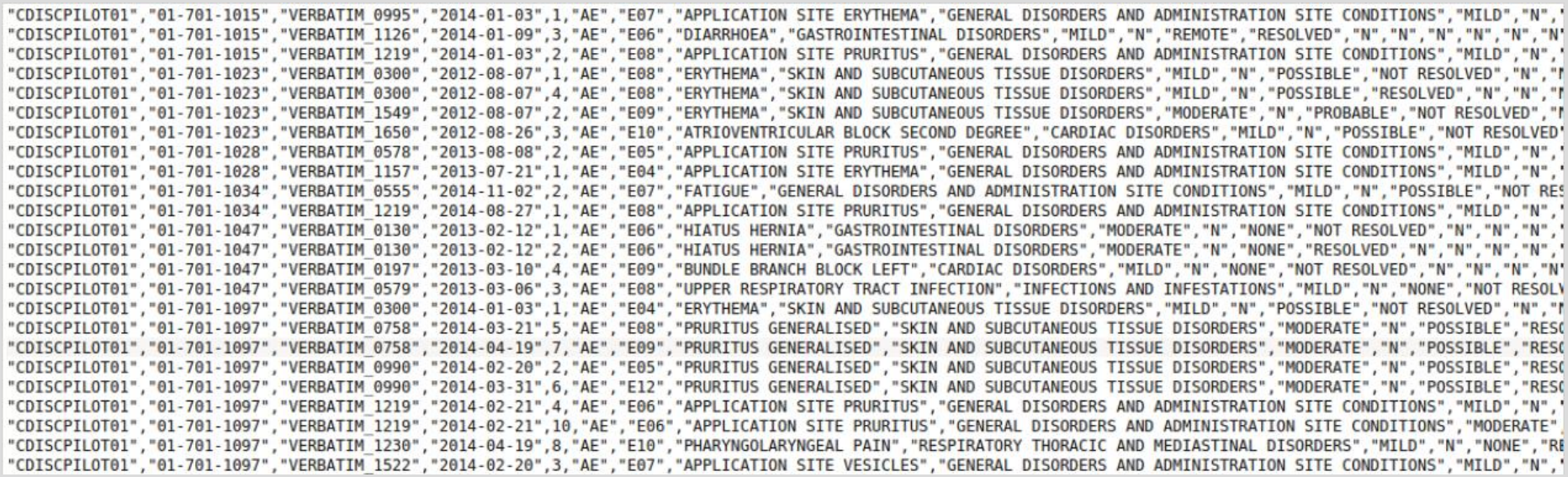
CIs should be carried in order to obtain the most conclusive results/data without compromising the health of subjects.

Motivational Application: Clinical Investigations

- Pharmaceutical companies (Sponsor), clinical research organizations (CRO), health institutions (HI) and government regulatory agencies collaborate in order to carry out Cis.

Motivational Application: Clinical Investigations

- Pharmaceutical companies (Sponsor), clinical research organizations (CRO), health institutions (HI) and government regulatory agencies collaborate in order to carry out Cis.



```
"CDISCPILOT01","01-701-1015","VERBATIM_0995","2014-01-03",1,"AE","E07","APPLICATION SITE ERYTHEMA","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
"CDISCPILOT01","01-701-1015","VERBATIM_1126","2014-01-09",3,"AE","E06","DIARRHOEA","GASTROINTESTINAL DISORDERS","MILD","N","REMOTE","RESOLVED","N","N","N","N","N","N"
"CDISCPILOT01","01-701-1015","VERBATIM_1219","2014-01-03",2,"AE","E08","APPLICATION SITE PRURITUS","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
"CDISCPILOT01","01-701-1023","VERBATIM_0300","2012-08-07",1,"AE","E08","ERYTHEMA","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MILD","N","POSSIBLE","NOT RESOLVED","N","N
"CDISCPILOT01","01-701-1023","VERBATIM_0300","2012-08-07",4,"AE","E08","ERYTHEMA","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MILD","N","POSSIBLE","RESOLVED","N","N","N
"CDISCPILOT01","01-701-1023","VERBATIM_1549","2012-08-07",2,"AE","E09","ERYTHEMA","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MODERATE","N","PROBABLE","NOT RESOLVED","N
"CDISCPILOT01","01-701-1023","VERBATIM_1650","2012-08-26",3,"AE","E10","ATRIOVENTRICULAR BLOCK SECOND DEGREE","CARDIAC DISORDERS","MILD","N","POSSIBLE","NOT RESOLVED"
"CDISCPILOT01","01-701-1028","VERBATIM_0578","2013-08-08",2,"AE","E05","APPLICATION SITE PRURITUS","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
"CDISCPILOT01","01-701-1028","VERBATIM_1157","2013-07-21",1,"AE","E04","APPLICATION SITE ERYTHEMA","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
"CDISCPILOT01","01-701-1034","VERBATIM_0555","2014-11-02",2,"AE","E07","FATIGUE","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","POSSIBLE","NOT RES
"CDISCPILOT01","01-701-1034","VERBATIM_1219","2014-08-27",1,"AE","E08","APPLICATION SITE PRURITUS","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
"CDISCPILOT01","01-701-1047","VERBATIM_0130","2013-02-12",1,"AE","E06","HIATUS HERNIA","GASTROINTESTINAL DISORDERS","MODERATE","N","NONE","NOT RESOLVED","N","N","N","
"CDISCPILOT01","01-701-1047","VERBATIM_0130","2013-02-12",2,"AE","E06","HIATUS HERNIA","GASTROINTESTINAL DISORDERS","MODERATE","N","NONE","RESOLVED","N","N","N","N","
"CDISCPILOT01","01-701-1047","VERBATIM_0197","2013-03-10",4,"AE","E09","BUNDLE BRANCH BLOCK LEFT","CARDIAC DISORDERS","MILD","N","NONE","NOT RESOLVED","N","N","N","N"
"CDISCPILOT01","01-701-1047","VERBATIM_0579","2013-03-06",3,"AE","E08","UPPER RESPIRATORY TRACT INFECTION","INFECTIONS AND INFESTATIONS","MILD","N","NONE","NOT RESOLV
"CDISCPILOT01","01-701-1097","VERBATIM_0300","2014-01-03",1,"AE","E04","ERYTHEMA","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MILD","N","POSSIBLE","NOT RESOLVED","N","N
"CDISCPILOT01","01-701-1097","VERBATIM_0758","2014-03-21",5,"AE","E08","PRURITUS GENERALISED","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MODERATE","N","POSSIBLE","RESO
"CDISCPILOT01","01-701-1097","VERBATIM_0758","2014-04-19",7,"AE","E09","PRURITUS GENERALISED","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MODERATE","N","POSSIBLE","RESO
"CDISCPILOT01","01-701-1097","VERBATIM_0990","2014-02-20",2,"AE","E05","PRURITUS GENERALISED","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MODERATE","N","POSSIBLE","RESO
"CDISCPILOT01","01-701-1097","VERBATIM_0990","2014-03-31",6,"AE","E12","PRURITUS GENERALISED","SKIN AND SUBCUTANEOUS TISSUE DISORDERS","MODERATE","N","POSSIBLE","RESO
"CDISCPILOT01","01-701-1097","VERBATIM_1219","2014-02-21",4,"AE","E06","APPLICATION SITE PRURITUS","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
"CDISCPILOT01","01-701-1097","VERBATIM_1219","2014-02-21",10,"AE","E06","APPLICATION SITE PRURITUS","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MODERATE",
"CDISCPILOT01","01-701-1097","VERBATIM_1230","2014-04-19",8,"AE","E10","PHARYNGOLARYNGEAL PAIN","RESPIRATORY THORACIC AND MEDIASTINAL DISORDERS","MILD","N","NONE","RE
"CDISCPILOT01","01-701-1097","VERBATIM_1522","2014-02-20",3,"AE","E07","APPLICATION SITE VESICLES","GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS","MILD","N","
```

Lots of data collected, typically in the order of gigabytes and poorly structured.

Motivational Application: Clinical Investigations

- Pharmaceutical companies (Sponsor), clinical research organizations (CRO), health institutions (HI) and government regulatory agencies collaborate in order to carry out Cis.

Procedures

Procedures are elaborated by specialists explaining how one should carry out CIs, so that the most conclusive data is collected and the health of subjects is not compromised.

Motivational Application: Clinical Investigations

- Pharmaceutical companies (Sponsor), clinical research organizations (CRO), health institutions (HI) and government regulatory agencies collaborate in order to carry out Cis.

Procedures

Regulations

"Any adverse experience associated with the use of the drug that is both serious and unexpected; […]
Each notification shall be made as soon as possible and *in no event later than 15 calendar days* after the sponsor's initial receipt of the information."

Adverse Events:

- unexpected collateral effects or even unrelated experiences
- governamental agencies (e.g. **FDA**) have to be informed

Motivational Application: Clinical Investigations

- Pharmaceutical companies (Sponsor), clinical research organizations (CRO), health institutions (HI) and government regulatory agencies collaborate in order to carry out Cis.

Procedures

Regulations

- Violations may also imply heavy penalties, both financial as well as of bad Public Relations:
  - CIs are rigorously monitored by government inspectors.
  - Health Institutions with record of deviations may be punished by the market and not being hired for carrying out future CIs.

Motivational Application: Clinical Investigations

- Pharmaceutical companies (Sponsor), clinical research organizations (CRO), health institutions (HI) and government regulatory agencies collaborate in order to carry out Cis.

Procedures

Regulations

Both procedures and regulations explicitly mention time and they mention actions with different outcomes.

Rewriting Framework – Local State Transition System (LSTS)

- FOL signature
- Configurations are multisets of facts:

$$\{\text{Nurse}(\text{Tom}, \text{id1}, \text{blood}), \text{Nurse}(\text{Sam}, \text{id2}, \text{blood})\}$$

- Actions are rewrite rules:

$$\text{Nurse}(\text{X}, \text{Y}, \text{blood}) \rightarrow \text{Nurse}(\text{blank}, \text{Y}, \text{blood})$$

$$\text{Lab}(\text{id}, \text{blood}) \rightarrow \text{Lab}(\text{id}, \text{testResults})$$

- Goals are multisets of facts:

$$\{\text{Doctor}(\text{testResults}, \text{Tom})\}$$

- Critical configurations are configurations that have to be avoided

$$\{\text{Lab}(\text{testResults}, \text{Tom})\} \qquad \{\text{Nurse}(\text{Tom}, \text{id1}, \text{blood}), \text{Nurse}(\text{Sam}, \text{id1}, \text{blood})\}$$

Previous results [Kanovich, Rowe, and Scedrov, CSF'07, CSF'09, Rowe PhD Dissertation UPENN'09]

Planning Problem

Is there a plan from an initial configuration to a configuration containing a goal such that no critical configuration is reached along the plan?

Example:
the test results of a patient should not be publicly leaked with the patient's name.

Previous results [Kanovich, Rowe, and Scedrov, CSF'07, CSF'09, Rowe PhD Dissertation UPENN'09]

Planning Problem

Is there a plan from an initial configuration to a configuration containing a goal such that no critical configuration is reached along the plan?

Example:
the test results of a patient should not be publicly leaked with the patient's name.

Assumption

Balanced actions, that is actions that have the same number of facts in their pre and post conditions.

Along a plan, configurations have the same number of facts.
Intuitively, agents have bounded memory.

Complexity Results

Balanced actions:

PSPACE-complete

Not necessarily balanced actions:

Undecidable

Rewriting Framework for Activities Subject to Regulations

Formal specification and verification
of activities such as CIs requires
branching, explicit time and fresh values.

Rewriting Framework for Activities Subject to Regulations

Formal specification and verification
of activities such as CIs requires
branching, explicit time and fresh values.

$$X_1, \ldots, X_n \rightarrow \exists \vec{n}. Y_1, \ldots, Y_m$$

- Plans may be exponentially long and involve exponentially many mutually distinct fresh values.

  [FAST 10] We fix a small number of nonce names and then reuse obsolete constants instead of updating with fresh constants.

Timestamps and Time Constraints

Motivation

$$\text{Time@}T,\ \text{Visit(I, ID, no)@}T_1 \mid \{T_1 - 5 \leq T \leq T_1 + 5\} \longrightarrow \text{Time@}T,\ \text{Visit(I, ID, yes)@}T$$

Timestamps and Time Constraints

Motivation

$$\text{Time@}T,\ \text{Visit(I, ID, no)@}T_1 \mid \{T_1 - 5 \leq T \leq T_1 + 5\} \longrightarrow \text{Time@}T,\ \text{Visit(I, ID, yes)@}T$$

Timestamps
Global Time

Time constraints
a scheduled visit has a tolerance of 5 days

Timestamps and Time Constraints

Motivation

$$\text{Time@}T,\ \text{Visit(I, ID, no)@}T_1 \mid \{T_1 - 5 \leq T \leq T_1 + 5\} \longrightarrow \text{Time@}T,\ \text{Visit(I, ID, yes)@}T$$

Timestamps
Global Time

Time constraints
a scheduled visit has a tolerance of 5 days

Other examples:

- time constraints often appear in legislation e.g. medical, financial
- timestamps are also used in protocols.

Timestamps and Time Constraints

Timed Goal Configurations

Data of the subjects have to be collected at the correct times:

Configuration $\{\text{Time@}T, \text{Data}(Id, 1)@T_1, \ldots, \text{Data}(Id, 25)@T_{25}\}$

Time constraints $T_i + 23 \leq T_{i+1} \leq T_i + 33$
and that $T > T_i$, for $1 \leq i \leq 25$

Timestamps and Time Constraints

Timed Goal Configurations

Data of the subjects have to be collected at the correct times:

Configuration $\{\text{Time@}T, \text{Data}(Id, 1)@T_1, \ldots, \text{Data}(Id, 25)@T_{25}\}$

Time constraints $T_i + 23 \leq T_{i+1} \leq T_i + 33$ and that $T > T_i$, for $1 \leq i \leq 25$

Timed Critical Configurations

regulatory agency is not informed within 15 days an unexpected event is detected:

Configuration $\{\text{Detect}(Id)@T_1, \text{Report}(Id)@T_2\}$

Time constraints $\{T_2 > T_1 + 15\}$

Branching

Motivation

$$Time@T, Test(Id, blank)@T_1 \longrightarrow \begin{array}{l} [\ Time@T, Test(Id, \mathbf{ok})@T\ ] \oplus \\ [Time@T, Test(Id, \mathbf{high})@T] \oplus \\ [\ Time@T, Test(Id, \mathbf{bad})@T\ ] \end{array}$$

There are three possible outcomes for the test: **ok**, **high** or **bad**.

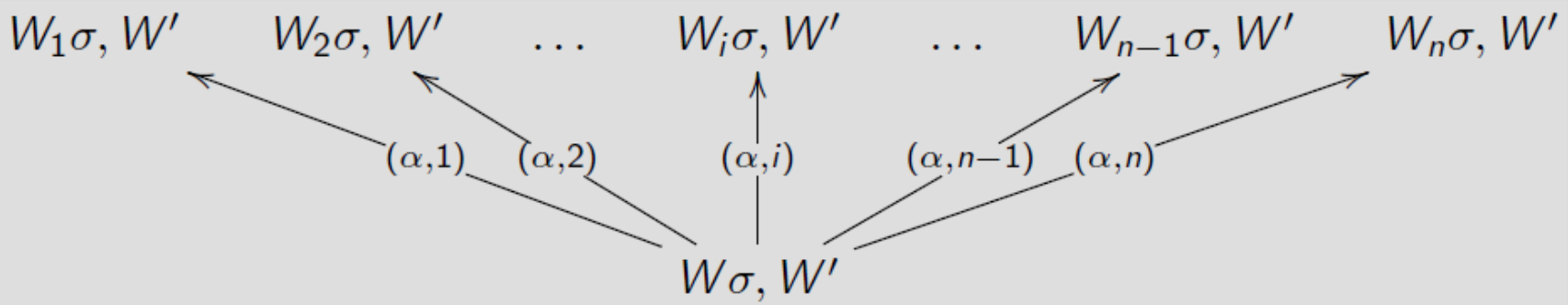
Other examples:

Often one needs to take different actions according to the outcome of an event:

e.g. in clinical trials: if the test result is bad, then repeat the test

Branching

Branching plans



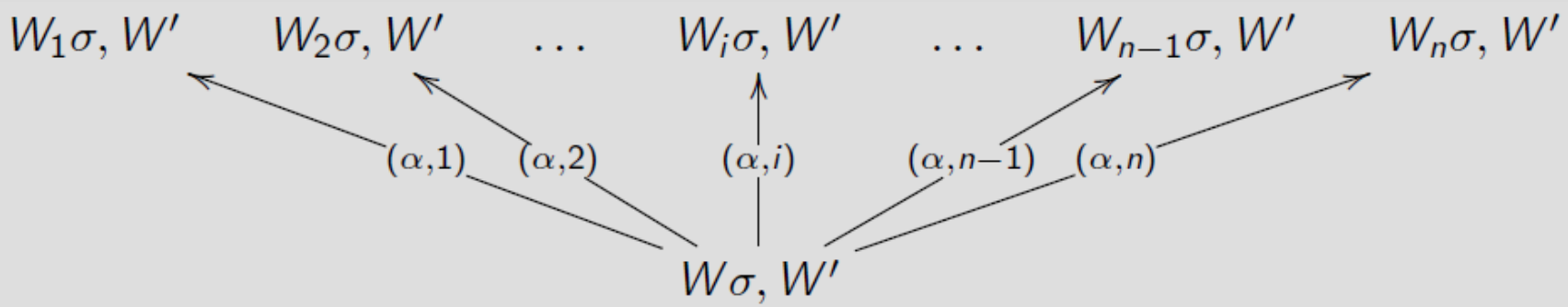
branching plan obtained by applying action α :

$$W \mid \Upsilon \longrightarrow [\exists \vec{x_1}.W_1] \oplus \cdots \oplus [\exists \vec{x_n}.W_n]$$

Here σ is a ground substitution for α's pre-condition W, while $W'_1\sigma, \ldots, W'_n\sigma$ are ground instantiations of α's post-conditions

Branching

Branching plans



Planning Problem

Given an initial configuration W and a finite set of goal and critical configurations a branching plan P is compliant if it does not contain any critical configuration and moreover if all branches of P lead from the initial configuration W to a goal configuration.

Assumptions

- Actions are balanced.
- Discrete time: timestamps are natural numbers.

  For example, a timestamp can denote the time when
  the fact was created or the time until which the fact is valid.

- Global time: *Time@T*
- Time tick action: *Time@T* → *Time@(T+1)*

Assumptions

- Time constraints are arithmetic comparisons of the form:

$$T_1 \circ T_2 + D, \text{ where } \circ \in \{<, \leq, =, \geq, >\}$$

where *D* is a natural number and T_1 and T_2 are time variables.

Time constraints are relative i.e. they are invariant with respect to time translation $t \rightarrow t + t_0$.

- Time constraints are attached to actions.

$$Time@T,W \mid \Upsilon \rightarrow \exists \mathbf{x}.Time@T,W'$$

- Timestamps of created facts in an action at the moment *T* are of the form: $T + D$, where *D* is a non-negative integer.

Assumptions

Relaxing assumptions

- Balanced actions

  When unbalanced actions are allowed the planning problem is undecidable [Kanovich, Rowe, and Scedrov, CSF'09]

Assumptions

Relaxing assumptions

- Balanced actions

- Time constraints: $T_1 \circ T_2 + D$, where $\circ \in \{<, \leq, =, \geq, >\}$

  New – if contraints with linear functions of 3 time variables are allowed
  the planning problem is undecidable:
  (reduction to the termination problem of two counter Minsky machine)

Assumptions

Relaxing assumptions

- Balanced actions
- Time constraints: $T_1 \circ T_2 + D$, where $\circ \in \{<, \leq, =, \geq, >\}$
- Timestamps of created facts in an action at the moment *T* :
  T + *D*, where *D* is a non-negative integer.

New – if timestamps with linear functions of time variables are allowed the planning problem is undecidable:
(reduction to the termination problem of two counter Minsky machine)

Summary of Results for Collaborative Systems

Planning Problem		
Balanced Actions	untimed systems	PSPACE-complete
	discrete time no branching	PSPACE-complete
	discrete time and branching	EXPTIME-complete
Actions not necessarily balanced		Undecidable

Above results also relate to systems with **fresh values**.

Handling the unboundedness of time

Challenge

Overcome the fact that the domain of timestamps is unbounded.

Example: a plan where the global time advances eagerly.

$$\mathrm{Time@0}, W \longrightarrow_{clock} \mathrm{Time@1}, W \longrightarrow_{clock} \mathrm{Time@2}, W \longrightarrow_{clock} \cdots$$

Handling the unboundedness of time

Solution

We propose an equivalence relation on configurations based on the time differences of facts:

Handling the unboundedness of time

Solution

We propose an equivalence relation on configurations based on the time differences of facts:

Truncated time difference of two facts $P@T_1$ *and* $Q@T_2$

$$\delta_{P,Q} = \begin{cases} T_2 - T_1, \text{ provided } T_2 - T_1 \leq D_{max} \\ \infty, \text{ otherwise} \end{cases}$$

where D_{max} *is an upper bound on the numbers in the planning problem.*

Handling the unboundedness of time

Solution

We propose an equivalence relation on configurations based on the time differences of facts:

Truncated time difference of two facts $P@T_1$ *and* $Q@T_2$

$$\delta_{P,Q} = \begin{cases} T_2 - T_1, \text{ provided } T_2 - T_1 \leq D_{max} \\ \infty, \text{ otherwise} \end{cases}$$

where D_{max} *is an upper bound on the numbers in the planning problem.*

Informally: Two configurations are equivalent if they have the same facts and the same truncated time differences.

Example

Assume $D_{max} = 3$, then the following configurations are equivalent:

$R@3$	$R@0$
$P@4$	$P@1$
$\mathrm{Time}@11$	$\mathrm{Time}@6$
$Q@12$	$Q@7$
$S@14$	$S@9$

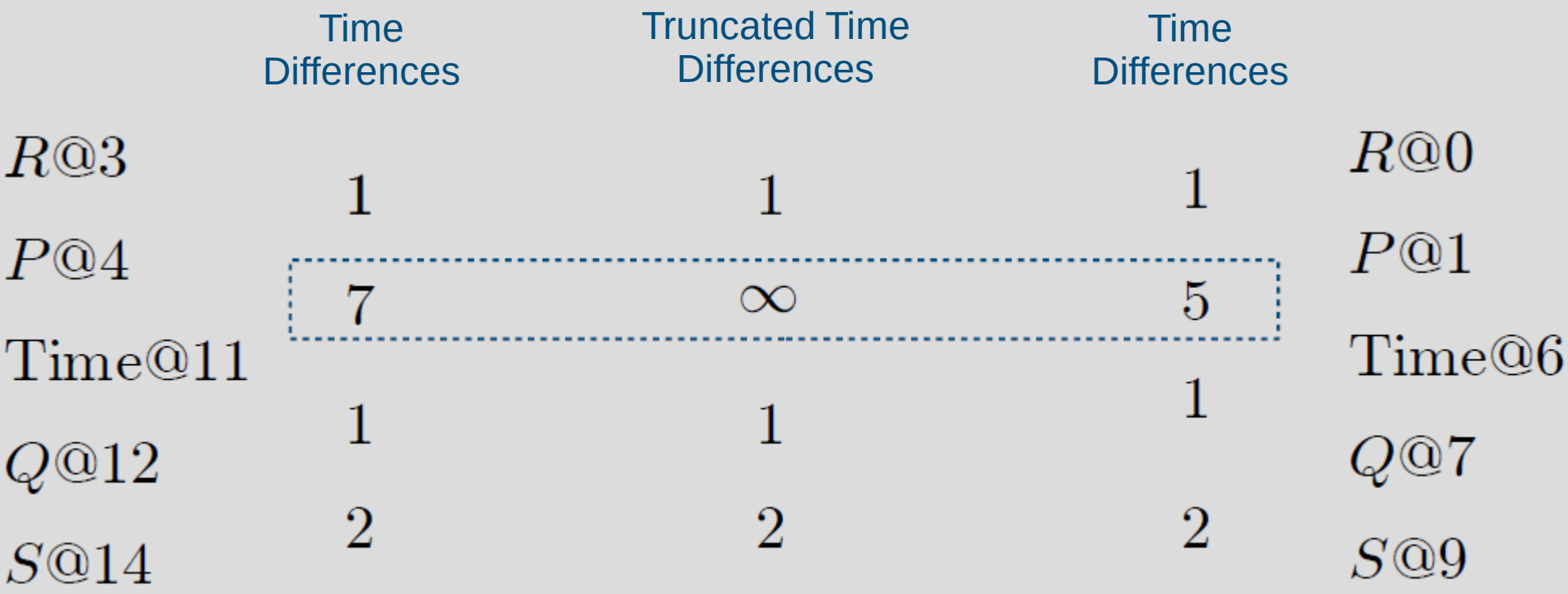
Example

Assume $D_{max} = 3$, then the following configurations are equivalent:

	Time Differences		Time Differences	
$R@3$	1	$R@0$	1	$R@0$
$P@4$	7	$P@1$	5	$P@1$
$\text{Time}@11$	1	$\text{Time}@6$	1	$\text{Time}@6$
$Q@12$	2	$Q@7$	2	$Q@7$
$S@14$		$S@9$		$S@9$

Example

Assume $D_{max} = 3$, then the following configurations are equivalent:



Example

Assume $D_{max} = 3$, then the following configurations are equivalent:

	Time Differences	Truncated Time Differences	Time Differences	
$R@3$				$R@0$
	1	1	1	
$P@4$				$P@1$
	7	∞	5	
$\mathrm{Time}@11$				$\mathrm{Time}@6$
	1	1	1	
$Q@12$				$Q@7$
	2	2	2	
$S@14$				$S@9$

Canonical form called δ-representation:

$$\langle R, 1, P, \infty, \mathrm{Time}, 1, Q, 2, S \rangle$$

Equivalent configurations and relative time constraints

Lemma: Let S and S' be equivalent configurations and let C be a relative time constraint. S satisfies C if and only if S' satisfies C.

Hence, if an action is applicable in the configuration S it will also be applicable in the configuration S'.
Moreover, if S is a goal (respectively, critical) configuration, then S' is also a goal (respectively, critical) configuration.

Actions preserve equivalences

Theorem: For a given planning problem any plan can be conceived as a plan over its δ-representations.

We only need to consider the planning problem with a bounded number of δ-representations with respect to:

- the number of facts in the initial configuration;
- the upper bound on the size of facts;
- the upper bound, D_{max}, of the numbers appearing in the theory.

Formal Semantics

We provide an encoding of our systems into linear logic with definitions.

Time constraint $T_1 \leq T_2 + d$ is encoded as

$$[\mathrm{Plus}(T_2, \ulcorner d \urcorner, T_2')] \otimes [T_1 \leq T_2']$$

$$\begin{array}{lcl} x \leq y & \triangleq & [x = \mathrm{zr}] \oplus \\ & & [\exists x'y'.(x = \mathrm{s}(x')) \otimes (y = \mathrm{s}(y')) \otimes (x' \leq y')] \\ \mathrm{Plus}(x, y, z) & \triangleq & [(x = \mathrm{zr} \otimes y = z)] \oplus \\ & & [\exists x'z'.((x = \mathrm{s}(x')) \otimes (z = \mathrm{s}(z')) \otimes \mathrm{Plus}(x', y, z')] \end{array}$$

Formal Semantics

We provide an encoding of our systems into linear logic with definitions.

There is a one-to-one correspondence between the set of plans and the set of (cut-free) focused proofs of the encoding.

Implementation

We also propose an encoding of our systems to the rewrite tool **Maude.**

Actions are encoded as rewrite rules:

```
crl[blood]: {(C:Conf)(time@T)(blood(Id,scheduled)@T)} =>
        {(C:Conf)(time@T)(blood(Id,positive)@T)} +
        {(C:Conf) (time@T) (blood(Id,negative)@T)}
if
 not (critical((C:Conf)(time@T)(blood(Id,positive)@T))) ∧
 not (critical((C:Conf)(time@T)(blood(Id,negative)@T)))
```

Implementation

We also propose an encoding of our systems to the rewrite tool **Maude.**

Critical and goal configurations are encoded as equational theories:

```
ceq critical((C:Conf)(time@T)(detected(Id,Num)@T1)
    (fda(Id,no,Num)@T2)) = true if T > T1 + 7
```

Implementation

We also propose an encoding of our systems to the rewrite tool **Maude.**

Planning: searching for a compliant plan is achieved by using Maude's search engine.

```
search in MODULE_NAME : I =>+ P:Plan
 such that goals(P:Plan) = true
```

Implementation

We also propose an encoding of our systems
to the rewrite tool **Maude.**

Monitoring: by using equational theory specifying critical configurations, one can detect deviations and send alarms to the responsible agents.

Data analysis: after a CI has been carried out, one could also use the actual plan carried out to study how CIs have been executed.

Future work

- Ways to translate protocols such as CI into our mathematical formalism for adequate human computer interfaces
- Systems with real time [FCS-FCC'14, POST'15]
- Verification of systems that require explicit real time:

  Distance Bounding Protocols

  Cyber-Physical Systems

Thank you.