

On the freeze operator in constraint LTL

Stéphane Demri

LSV, ENS de Cachan

Joint work with Ranko Lazić and David Nowak

Constraint systems

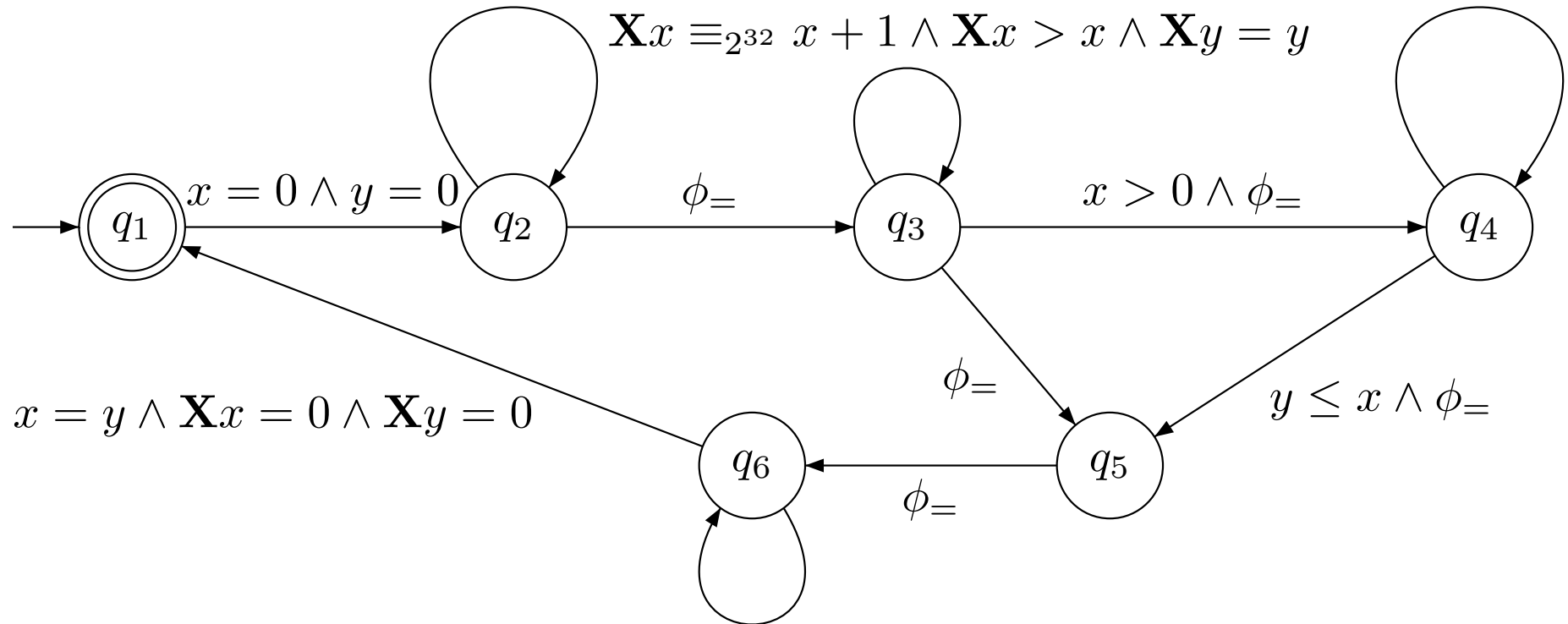
- Constraint system: $\mathcal{D} = \langle D, (R_\alpha)_{\alpha \in I} \rangle$.
- Interpretation domains of program variables.
- Atomic \mathcal{D} constraint: $R(x_1, \dots, x_t), x_i \in \text{VarSet}$.
- A D -valuation $v : \text{VarSet} \rightarrow D$.
- Examples: $\langle \mathbb{N}, =, < \rangle, \langle \mathbb{N}, =, \text{succ} \rangle, \langle \mathbb{R}, =, < \rangle, \langle \mathbb{Z}, =, < \rangle, \langle \{0, 1\}^*, \subset, = \rangle, \langle \mathbb{Z}, (R_{\phi(x_1, \dots, x_n)})_{\phi(x_1, \dots, x_n) \in \text{Presburger}} \rangle \dots$

D-automata

$$\mathbf{X}x \equiv_{2^{32}} x + 1 \wedge \mathbf{X}x > x \wedge \mathbf{X}y = y$$

$$y \leq x \wedge \mathbf{X}y \equiv_{2^{32}} y + 1 \wedge \dots$$

$$\mathbf{X}x \equiv_{2^{32}} x + 1 \wedge \mathbf{X}x > x \wedge \mathbf{X}y = y$$



$$\mathbf{X}y \leq x, \mathbf{X}y \equiv_{2^{32}} y + 1 \wedge \mathbf{X}y > y \wedge \mathbf{X}x = x$$

Logics over constraint systems

- Design of temporal logics for model-checking \mathcal{D} -automata.
- Which properties of the constraint system lead to decidability?
- Which ingredients of temporal logics lead to undecidability?
- Which techniques of the temporal logic L can be used for $L(\mathcal{D})$?

LTL over constraint systems

- Atomic term constraint $R(\mathbf{X}^{n_1}x_1, \dots, \mathbf{X}^{n_t}x_t)$.
- $\mathbf{X}^i x$ interpreted as the value of x in the i th next state.
- $\phi ::= R(\mathbf{X}^{n_1}x_1, \dots, \mathbf{X}^{n_t}x_t) \mid \neg\phi \mid \dots$ the rest as for LTL.
- Models: $\sigma : \mathbb{N} \rightarrow (\text{VarSet} \rightarrow D)$.
- $\sigma, j \models R(\mathbf{X}^{n_1}x_1, \dots, \mathbf{X}^{n_t}x_t)$ iff
value of x_1 in the $j+n_1$ th state
 $(\overbrace{\sigma(j+n_1)(x_1)}^{\text{value of } x_1 \text{ in the } j+n_1 \text{th state}}, \dots, \sigma(j+n_t)(x_t)) \in R$

i.e. values at different states can be compared.

LTL as a fragment of CLTL($\{0, 1\}, =$)

- $\{p_2, p_3\} \cdot \{p_3\} \cdot \{p_1, p_3\} \dots \models \mathbf{F}(p_1 \wedge p_3)$

\rightsquigarrow

$$\begin{array}{l} x_1 \quad 0 \quad 0 \quad \mathbf{1} \quad \dots \\ x_2 \quad 1 \quad 0 \quad 0 \quad \dots \quad \models \mathbf{F}(x_1 = 1 \wedge x_3 = 1) \\ x_3 \quad 1 \quad 1 \quad \mathbf{1} \quad \dots \end{array}$$

- $p_i \approx (x_i = 1) \quad p_i \Leftrightarrow \mathbf{X}\mathbf{X}p_j \approx x_i = \mathbf{X}^2x_j.$

CLTL(\mathcal{D}) problems

- Satisfiability problem for CLTL(\mathcal{D}):
instance: a CLTL(\mathcal{D}) formula ϕ ,
question: is there a model σ such that $\sigma \models \phi$?
- Model-checking problem for CLTL(\mathcal{D}):
instance: A \mathcal{D} -automaton \mathcal{A} and a CLTL(\mathcal{D}) formula ϕ ,
question: are there a symbolic ω -word $v = \phi_0, \phi_1, \dots$ accepted by \mathcal{A} , a model σ (a realization of v) such that $\sigma \models \phi$ and for every $i \geq 0$, $\sigma, i \models \phi_i$?
- Standard equivalence between these problems.

Constraint versions of LTL

- For every finite \mathcal{D} , $\text{CLTL}(\mathcal{D})$ is in PSPACE.
- $\text{CLTL}(D, <, =)$ is PSPACE-complete for every $D \in \{\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}\}$.
- LTL over integer periodicity constraints + constraints of the form $x < y$ over \mathbb{Z} is also PSPACE-complete.
- $\text{CLTL}(\mathbb{N}, =, +1)$ is undecidable but flat LTL over Presburger constraints is decidable [Comon&Cortier00].
Different from Presburger LTL from [Bouajjani et al.95].
- Open problem: decidability status of $\text{CLTL}(\{0, 1\}^*, \subseteq)$ with either the prefix or the subword relation.

Extensions of the logical language

- Past-time operators.
Thanks to [Gastin&Kuske03] most PSPACE results can be extended by adding a finite number of MSO-definable operators.
- Branching-time temporal logics.
Model-checking for CTL extension of $\text{CLTL}(\mathbb{Z}, <, =)$ + constants is already undecidable [Cerans94].
- First-order features.
TPTL [Alur&Henzinger94] with freeze operator is decidable.

Adding the freeze operator

- $\text{VarSet} = \text{FleVarSet}$ (flexible variables) \cup RigVarSet (rigid variables).
- Unary $\downarrow_{y=\mathbf{X}^j x}$ with $y \in \text{RigVarSet}$, $x \in \text{FleVarSet}$.
- Environment $\rho: \text{RigVarSet} \rightarrow D$.
- Models $\sigma: \mathbb{N} \rightarrow (\text{FleVarSet} \rightarrow D)$.
- $\sigma \models_{\rho} \downarrow_{y=\mathbf{X}^n x} \phi$ iff $\sigma \models_{\rho[y \mapsto \sigma(n)(x)]} \phi$.
- $\sigma \models_{\rho} R(t_1, \dots, t_n)$ iff $(\llbracket t_1 \rrbracket_{\sigma, \rho}, \dots, \llbracket t_n \rrbracket_{\sigma, \rho}) \in R$ with

$$\begin{aligned} \llbracket \mathbf{X}^n x \rrbracket_{\sigma, \rho} &= \sigma(n)(x) && \text{if } x \text{ is in FleVarSet} \\ \llbracket y \rrbracket_{\sigma, \rho} &= \rho(y) && \text{if } y \text{ is in RigVarSet} \end{aligned}$$

Examples

- TPTL is exactly the fragment of the logic $\text{CLTL}^\downarrow(\mathcal{D})$ where
 - $D = \mathbb{N}$ and the only flexible variable is t (time);
 - the predicates of \mathcal{D} are the following:
 - $(x \leq c)_{c \in \mathbb{Z}}, (x \leq y + c)_{c \in \mathbb{Z}},$
 - $(x \equiv_d c)_{c, d \in \mathbb{N}}, (x \equiv_d y + c)_{c, d \in \mathbb{N}},$
 - the formulae are of the form $\mathbf{G}(t \leq \mathbf{X}t) \wedge \mathbf{GF}(t < \mathbf{X}t) \wedge \phi$ with the freeze quantifier used with bindings of the form $\downarrow_{x=t}$.
- $\text{CLTL}^\downarrow(\text{IPC}^+)$ defined over the constraints π of the form

$$x < d \mid x = d \mid x \equiv_k y + c \mid \neg\pi \mid \pi_1 \wedge \pi_2 \mid \exists x \pi$$

with variables interpreted in \mathbb{Z} is EXPSPACE-complete [Demri04] (no equality “ $x = y$ ”).

Freezing the current value is enough

- **Proposition.** For any formula ϕ of $\text{CLTL}^\downarrow(\mathcal{D})$, there exists an equivalent formula ϕ' such that:
 - any occurrence of \downarrow in ϕ' is of the form $\downarrow_{y=x}$,
 - $\text{FleVars}(\phi') = \text{FleVars}(\phi)$ and $\text{RigVars}(\phi') = \text{RigVars}(\phi)$.
- Reduction for formulae $\downarrow_{y=\mathbf{X}^n x} \psi$.
- Proof by structural induction on $\langle |\psi|, n \rangle$.
- Until case:

$$\begin{aligned} & \downarrow_{y=\mathbf{X}^{n+1}x} \psi_1 \mathbf{U} \psi_2 \\ \equiv & \downarrow_{y=\mathbf{X}^{n+1}x} \psi_2 \vee (\psi_1 \wedge \mathbf{X} \psi_1 \mathbf{U} \psi_2) \\ \equiv & (\downarrow_{y=\mathbf{X}^{n+1}x} \psi_2) \vee ((\downarrow_{y=\mathbf{X}^{n+1}x} \psi_1) \wedge \mathbf{X} \downarrow_{y=\mathbf{X}^n x} \psi_1 \mathbf{U} \psi_2) \end{aligned}$$

Atomic formulae with rigid variables

For any formula ϕ of $\text{CLTL}^\downarrow(\mathcal{D})$, there exists an equivalent formula ψ such that:

- atomic formulae in ψ contain only rigid variables,
- if any occurrence of \downarrow in ϕ is of the form $\downarrow_{y=x}$, then the same is true of ψ ,
- $\text{FleVars}(\psi) = \text{FleVars}(\phi)$,
- if k is the maximum number, over all atomic formulae in ϕ , of distinct terms of the form $\mathbf{X}^n x$ with $x \in \text{FleVarSet}$, then $|\text{RigVars}(\psi)| \leq |\text{RigVars}(\phi)| + k$.

Undecidable variants

- The following variants of TPTL are undecidable [Alur&Henzinger94]
 - without the monotonicity conditions on time sequences or,
 - with the addition of the multiplication by 2 or,
 - by replacing the time domain by \mathbb{Q} .
- $\text{CLTL}^\downarrow(\mathbb{N}, <, =)$ with past-time operator F^{-1} is undecidable.
- $\text{CLTL}^\downarrow(\mathbb{N}, =)$ restricted to 1 rigid variable, 4 flexible variables and the operators X, X^{-1}, F, F^{-1} is already undecidable, consequence of [David04].

Other logics with freeze (I)

- \downarrow_x in hybrid logics [Blackburn&Seligman95, Goranko96].
 - $\downarrow_x \phi$: ϕ holds true in the variant model where x is true only at the current state.
 - Every reachable state can be visited inf. often: $\forall G \downarrow_x \exists X F x$.
- LTL with past-time operators and Now [Laroussinie et al.02].

Other logics with freeze (II)

- Repeated Hybrid Quantified LTL [French03].
 - Model (μ, σ) with $\mu : \mathbb{N} \rightarrow S$ and $\sigma : S \rightarrow 2^{\text{AP}}$.
 - $(\mu, \sigma), i \models_{\downarrow p} \phi$ iff $(\mu, \sigma'), i \models \phi$ where σ' is the p -variant of σ in which p belongs only to $\sigma'(\mu(i))$.
 - RHLTL with $\mathbf{F}, \mathbf{X}, \dots$ equivalent to $\text{CLTL}^{\downarrow}(\mathbb{N}, =)$ with $\mathbf{F}, \mathbf{X}, \dots$ restricted to one flexible variable.
 - **Corollary.** $\text{CLTL}^{\downarrow}(\mathbb{N}, =)$ restricted with 2 rigid variables and the temporal operators $\mathbf{X}, \mathbf{X}^{-1}, \mathbf{F}, \mathbf{F}^{-1}$ is undecidable.

First-order logics

- First-order temporal logics [Gabbay et al.03].
 - Flexible variable $x \rightsquigarrow$ monadic P_x interpreted by singleton.
 - $T(x = x') = \exists y P_x(y) \wedge P_{x'}(y)$ $T(\downarrow_{y=x} \phi) = \exists y P_x(y) \wedge T(\phi)$.
 - $\text{CLTL}^\downarrow(\mathbb{N}, =)$ with one rigid variable can be encoded in monodic fragment with 2 individual variables, monadic predicate symbols, equality.
- Logics on words with data [David04, Bojańczyk et al.05].
 - Decidability of $\text{FO2}(\sim, <, +1)$ [Bojańczyk et al.05].
 - $\text{CLTL}^\downarrow(\mathbb{N}, =)$ can be easily encoded in $\text{FO}(\sim, <, +1)$.
 - See also register automata [Kaminski&Francez94] and data automata [Bouyer et al 03].

Finite domain \mathcal{D}

- **Theorem.** \mathcal{D} constraint system with equality such that $|D| \geq 2$. Satisfiability for $\text{CLTL}^\downarrow(\mathcal{D})$ is EXPSPACE-hard.
- Reduction from the 2^n corridor tiling problem. Comparison of variables of temporal distance 2^n is possible.
- **Theorem.** \mathcal{D} finite constraint system. Satisfiability for $\text{CLTL}^\downarrow(\mathcal{D})$ is in EXPSPACE.

Sketch of the proof (I)

- From $D = \{d_1, \dots, d_l\}$ define $\mathcal{D}' = \langle D, P_1, \dots, P_l \rangle$ such that $P_i = \{d_i\}$. We write $x = d_i$ instead of $P_i(x)$.
- Translation from $\text{CLTL}^\downarrow(\mathcal{D})$ into $\text{CLTL}(\mathcal{D}')$:
 - T is homomorphic for the Boolean and temporal operators,
 - $\mathsf{T}(\mathsf{R}(\alpha_1, \dots, \alpha_n)) = (\bigvee_{R(d_{i_1}, \dots, d_{i_n})} (\alpha_1 = d_{i_1} \wedge \dots \wedge \alpha_n = d_{i_n}))$,
 - $\mathsf{T}(\downarrow_{x'=\alpha} \psi) = \bigwedge_{d_i \in D} (\alpha = d_i) \Rightarrow \mathsf{T}(\psi)^{x'=d_i}$, where $\mathsf{T}(\psi)^{x'=d_i}$ is obtained from $\mathsf{T}(\psi)$ by replacing every occurrence of $x' = d_j$ with $j \neq i$ by \perp and every occurrence of $x' = d_i$ by \top .
- The last clause causes an exponential blow up.

Sketch of the proof (II)

- ϕ is $\text{CLTL}^\downarrow(\mathcal{D})$ satisfiable iff $\mathsf{T}(\phi)$ is $\text{CLTL}(\mathcal{D}')$ satisfiable.
- $\text{CLTL}(\mathcal{D}')$ is PSPACE-complete.
- $\text{CLTL}^\downarrow(\mathcal{D})$ is in EXPSPACE.
- \downarrow -height: maximal number of \downarrow in a branch of the formula tree.
- **Corollary.** For every $k \geq 0$, the satisfiability problem for $\text{CLTL}^\downarrow(\mathcal{D})$ restricted to formulae of \downarrow -height k is in PSPACE.

Flat fragment

- Flat $\text{CLTL}^\downarrow(\mathcal{D})$: restriction of $\text{CLTL}^\downarrow(\mathcal{D})$ where, for any subformula $\psi_1 \mathbf{U} \psi_2$, if it is positive then \downarrow does not occur in ψ_1 , and if it is negative then \downarrow does not occur in ψ_2 .

- Formulae below belong to the flat fragment:

$$\downarrow_{x'=x} \mathbf{F}(x' < y) \quad \neg \mathbf{G} \downarrow_{y=x} \mathbf{XG}x \neq y$$

- $\text{CLTL}(\mathcal{D})$ is in the flat fragment of $\text{CLTL}^\downarrow(\mathcal{D})$.
- Flat $\text{CLTL}^\downarrow(\mathbb{N}, =)$ is strictly more expressive than $\text{CLTL}(\mathbb{N}, =)$.

Reduction to $CLTL(\mathcal{D})$

- Translation from flat $CLTL^\downarrow(\mathcal{D})$ into $CLTL(\mathcal{D})$:
 - $T(c) \stackrel{\text{def}}{=} c'$ where c' is obtained from c by replacing each rigid variable y by y_{new} ,
 - T is homomorphic for Boolean and temporal operators,
 - $T(\downarrow_{y=\mathbf{X}^n x} \psi) \stackrel{\text{def}}{=} y^{\text{new}} = \mathbf{X}^n x \wedge \mathbf{G}(y^{\text{new}} = \mathbf{X}y^{\text{new}}) \wedge T(\psi)$.
- **Lemma.** \mathcal{D} constraint system with equality. For any formula ϕ of the flat fragment of $CLTL^\downarrow(\mathcal{D})$, ϕ is $CLTL^\downarrow(\mathcal{D})$ satisfiable iff $T(\phi)$ is $CLTL(\mathcal{D})$ satisfiable.
- **Corollary.** Flat fragments of $CLTL^\downarrow(\mathbb{Z}, <, =)$, $CLTL^\downarrow(\mathbb{N}, <, =)$, $CLTL^\downarrow(\mathbb{R}, <, =)$, and $CLTL^\downarrow(\mathcal{D})$ with \mathcal{D} finite are PSPACE-complete.

Σ_1^1 -completeness of $CLTL^\downarrow(\mathbb{N}, =)$

- $CLTL^\downarrow(\mathbb{N}, =)$: minimal pure-future constrained version of LTL with unrestricted freeze operator.
- Reduction of the rec. problem for nondet. 2-counter machines.
- Instructions of the form

$l : C_i := C_i + 1; \text{ goto } l' \text{ or goto } l''$

$l : C_i := C_i - 1; \text{ goto } l' \text{ or goto } l''$

$l : \text{ if } C_i = 0 \text{ then goto } l' \text{ else goto } l''$

- **Theorem.** D infinite set. Satisfiability for $CLTL^\downarrow(D, =)$ restricted to one flexible variable and two rigid variables is Σ_1^1 -hard.

Encoding of configurations

Configuration $\langle l, c_1, c_2 \rangle$ encoded by a sequence of the form

$$ddd'd \underbrace{\dots d' \dots}_n f_1^1 \dots f_{c_1}^1 eee'e'' f_1^2 \dots f_{c_2}^2$$

where:

- (i) the only two pairs of consecutive elements which are equal are dd and ee , and also $f_{c_2}^2$ is distinct from the first element in the encoding of the next configuration;
- (ii) $e \neq e''$;
- (iii) after the first 4 elements, there is a sequence of n (number of instructions) elements, and only the l^{th} equals d' ;
- (iv) $f_1^i, \dots, f_{c_i}^i$ are mutually distinct.

Global encoding

$$\phi_n^{glob} \stackrel{\text{def}}{=} \mathbf{G}(\text{start}_d \Rightarrow \psi_n^1 \wedge \text{start}_e \Rightarrow \psi_n^2)$$

in $dd'd \dots d' \dots$ two consecutive values are distinct

$$\psi_n^1 \stackrel{\text{def}}{=} \left(\bigwedge_{i=1}^{n+3} \mathbf{X}^i x \neq \mathbf{X}^{i+1} x \right) \wedge$$

in $\dots d' \dots$ exactly one value equals d'

$$\left(\bigvee_{l=1}^n \mathbf{X}^{2l} x = \mathbf{X}^{l+3} x \wedge \left(\bigwedge_{j=1}^{l-1} \mathbf{X}^{2j} x \neq \mathbf{X}^{j+3} x \wedge \bigwedge_{j=l+1}^n \mathbf{X}^{2j} x \neq \mathbf{X}^{j+3} x \right) \right)$$

$f_1^1 \dots f_{c_1}^1$ mutually distinct

$$\mathbf{X}^{n+4} (\psi^{dist} \mathbf{U} \text{start}_e)$$

$f_1^2 \dots f_{c_2}^2$ mutually distinct

$$\psi_n^2 \stackrel{\text{def}}{=} \left(\bigwedge_{i=1}^3 \mathbf{X}^i x \neq \mathbf{X}^{i+1} x \right) \wedge \mathbf{X}^4 (\psi^{dist} \mathbf{U} \text{start}_d)$$

More formulae

- $\psi^{dist} \stackrel{\text{def}}{=} \neg \text{start}_{d \vee e} \wedge \downarrow_{y=x} \mathbf{X}((\neg \text{start}_{d \vee e} \wedge x \neq y) \mathbf{U} \text{start}_{d \vee e})$.
- $l : C_2 := C_2 - 1; \text{ goto } l' \text{ or } \text{ goto } l''$.

$$\mathbf{G}((\text{start}_d \wedge \mathbf{X}^2 x = \mathbf{X}^{l+3} x) \Rightarrow \mathbf{X}^{n+4} (\chi_{eq}^1 \wedge (\neg \text{start}_{d \vee e} \mathbf{U} (\text{start}_e \wedge \mathbf{X}^4 (\chi_{dec}^2 \wedge (\neg \text{start}_{d \vee e} \mathbf{U} (\text{start}_d \wedge (\mathbf{X}^2 x = \mathbf{X}^{l'+3} x \vee \mathbf{X}^2 x = \mathbf{X}^{l''+3} x))))))))))$$

- You do not want to see χ_{eq}^1 and χ_{dec}^2 !!

Corollaries

- **Corollary.** RHLTL with temporal operators \mathbf{U} and \mathbf{X} and without propositional variables is Σ_1^1 -complete.
- **Corollary.** TPTL without monotonicity is Σ_1^1 -complete even without propositional variables and with only equality constraints.

Some open problems

- Semantical restriction: to use $\downarrow_{x=t}$ only for t bounded-reversal?
- Decidability status of $\text{CLTL}^{\downarrow}(\{0, 1\}^*, \subset)$.
- Relationships with other formalisms, see e.g. [Bojańczyk et al.05].
- Decidability status of syntactic fragments.