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: $R(x_1, \ldots, x_t), x_i \in \text{VarSet}$.

- A $D$-valuation $v : \text{VarSet} \rightarrow D$.

- Examples: $\langle \mathbb{N}, =, < \rangle$, $\langle \mathbb{N}, =, \text{succ} \rangle$, $\langle \mathbb{R}, =, < \rangle$, $\langle \mathbb{Z}, =, < \rangle$, $\langle \{0, 1\}^*, \subseteq, = \rangle$, $\langle \mathbb{Z}, (R_{\phi(x_1, \ldots, x_n)})_{\phi(x_1, \ldots, x_n) \in \text{Presburger}} \rangle$ · · ·
$D$-automata

$Xx \equiv_{232} x + 1 \land Xx > x \land Xy = y$

$x = 0 \land y = 0$

$q_1$ $q_2$ $q_3$ $q_4$

$Xx \equiv_{232} x + 1 \land Xx > x \land Xy = y$

$q_6$ $q_5$

$y \leq x \land Xy \equiv_{232} y + 1 \land \ldots$

$x = y \land Xx = 0 \land Xy = 0$

$Xy \leq x, Xy \equiv_{232} y + 1 \land Xy > y \land Xx = x$
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 $R(\mathbf{X}^{n_1}x_1, \ldots, \mathbf{X}^{n_t}x_t)$.

- $\mathbf{X}^i x$ interpreted as the value of $x$ in the $i$th next state.

- $\phi ::= R(\mathbf{X}^{n_1}x_1, \ldots, \mathbf{X}^{n_t}x_t) \mid \neg \phi \mid \ldots$ the rest as for LTL.

- Models: $\sigma : \mathbb{N} \rightarrow (\text{VarSet} \rightarrow D)$.

- $\sigma, j \models R(\mathbf{X}^{n_1}x_1, \ldots, \mathbf{X}^{n_t}x_t)$ iff
  value of $x_1$ in the $j+n_1$th state
  $$(\sigma(j+n_1)(x_1), \ldots, \sigma(j+n_t)(x_t)) \in R$$

  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\} \ldots \models \text{F}(p_1 \land p_3)

\implies

\begin{align*}
x_1 & \quad 0 \quad 0 \quad 1 \quad \ldots \\
x_2 & \quad 1 \quad 0 \quad 0 \quad \ldots \quad \models \text{F}(x_1 = 1 \land x_3 = 1) \\
x_3 & \quad 1 \quad 1 \quad 1 \quad \ldots
\end{align*}

- \ p_i \approx (x_i = 1) \quad p_i \iff \text{XX}p_j \approx x_i = \text{X}^2 x_j.
CLTL(\(\mathcal{D}\)) problems

- Satisfiability problem for CLTL(\(\mathcal{D}\)):
  instance: a CLTL(\(\mathcal{D}\)) formula \(\phi\),
  question: is there a model \(\sigma\) such that \(\sigma \models \phi\)?

- Model-checking problem for CLTL(\(\mathcal{D}\)):
  instance: A \(\mathcal{D}\)-automaton \(A\) and a CLTL(\(\mathcal{D}\)) formula \(\phi\),
  question: are there a symbolic \(\omega\)-word \(v = \phi_0, \phi_1, \ldots\) accepted by \(A\), a model \(\sigma\) (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 $D$, CLTL($D$) is in PSPACE.

- 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.

- 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 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 CLTL(\(\mathbb{Z}, <, =\)) + constants is already undecidable [Cerans94].

- First-order features. TPTL [Alur&Henzinger94] with freeze operator is decidable.
Adding the freeze operator

- \( \text{VarSet} = \text{FleVarSet} \ (\text{flexible variables}) \cup \text{RigVarSet} \ (\text{rigid variables}) \).

- \( \text{Unary} \downarrow_{y = x^{j}x} \) with \( y \in \text{RigVarSet}, \ x \in \text{FleVarSet} \).

- Environment \( \rho: \text{RigVarSet} \to D \).

- Models \( \sigma: \mathbb{N} \to (\text{FleVarSet} \to D) \).

- \( \sigma \models_{\rho} \downarrow_{y = x^n x} \phi \iff \sigma \models_{\rho[y \mapsto \sigma(n)(x) \phi]} \).

- \( \sigma \models_{\rho} R(t_1, \ldots, t_n) \iff ([t_1]_{\sigma, \rho}, \ldots, [t_2]_{\sigma, \rho}) \in R \) with

\[
[X^n x]_{\sigma, \rho} = \sigma(n)(x) \quad \text{if } x \text{ is in } \text{FleVarSet} \\
[y]_{\sigma, \rho} = \rho(y) \quad \text{if } y \text{ is in } \text{RigVarSet}
\]
Examples

• TPTL is exactly the fragment of the logic $\text{CLTL}^\downarrow(D)$ where
  
  - $D = \mathbb{N}$ and the only flexible variable is $t$ (time);
  - the predicates of $D$ 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 $G(t \leq Xt) \land GF(t < Xt) \land \phi$
    with the freeze quantifier used with bindings of the form $\downarrow x=t$.

• $\text{CLTL}^\downarrow(\text{IPC}^+)$ defined over the constraints $\pi$ of the form

\[
x < d \mid x = d \mid x \equiv_k y + c \mid \neg \pi \mid \pi_1 \land \pi_2 \mid \exists x \pi
\]

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

• Proposition. For any formula \( \phi \) of CLTL\(^\downarrow\)(D), there exists an equivalent formula \( \phi' \) such that:
  
  – any occurrence of \( \downarrow \) in \( \phi' \) 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:

\[
\downarrow y=\mathbf{x}^{n+1} x \psi_1 \mathbf{U} \psi_2 \\
\equiv \downarrow y=\mathbf{x}^{n+1} x \psi_2 \lor (\psi_1 \land \mathbf{X} \psi_1 \mathbf{U} \psi_2) \\
\equiv (\downarrow y=\mathbf{x}^{n+1} x \psi_2) \lor ((\downarrow y=\mathbf{x}^{n+1} x \psi_1) \land \mathbf{X} \downarrow y=\mathbf{x}^n x \psi_1 \mathbf{U} \psi_2)
\]
Atomic formulae with rigid variables

For any formula $\phi$ of CLTL$\downarrow(D)$, there exists an equivalent formula $\psi$ such that:

- atomic formulae in $\psi$ contain only rigid variables,

- if any occurrence of $\downarrow$ in $\phi$ is of the form $\downarrow y=x$, then the same is true of $\psi$,

- $\text{FleVars}(\psi) = \text{FleVars}(\phi)$,

- if $k$ is the maximum number, over all atomic formulae in $\phi$, of distinct terms of the form $X^n x$ with $x \in \text{FleVarSet}$, then
  $|\text{RigVars}(\psi)| \leq |\text{RigVars}(\phi)| + k$. 

On the freeze operator in constraint LTL – p. 13
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 \( \mathbb{Q} \).

- CLTL\(\downarrow(N, <, =)\) with past-time operator \( F^{-1} \) is undecidable.

- CLTL\(\downarrow(N, =)\) 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].
  
  – $\downarrow x \phi$: $\phi$ holds true in the variant model where $x$ is true only at the current state.

  – Every reachable state can be visited inf. often: $\forall G \downarrow x \exists XF x$.

• LTL with past-time operators and $\text{Now}$ [Laroussinie et al.02].
Other logics with freeze (II)

- Repeated Hybrid Quantified LTL [French03].
  - Model \((\mu, \sigma)\) with \(\mu : \mathbb{N} \to S\) and \(\sigma : S \to 2^{AP}\).
  - \((\mu, \sigma), i \models \downarrow_p \phi \iff (\mu, \sigma'), i \models \phi\) where \(\sigma'\) is the \(p\)-variant of \(\sigma\) in which \(p\) belongs only to \(\sigma'(\mu(i))\).
  - RHLTL with \(F, X, \ldots\) equivalent to \(\text{CLTL}^\downarrow(\mathbb{N}, =)\) with \(F, X, \ldots\) restricted to one flexible variable.

- Corollary. \(\text{CLTL}^\downarrow(\mathbb{N}, =)\) restricted with 2 rigid variables and the temporal operators \(X, X^{-1}, F, F^{-1}\) is undecidable.
First-order logics

- First-order temporal logics [Gabbay et al.03].
  - Flexible variable $x \leadsto$ monadic $P_x$ interpreted by singleton.
  - $T(x = x') = \exists y P_x(y) \land P_{x'}(y)$  
    $T(\downarrow y=x \phi) = \exists y P_x(y) \land T(\phi)$.
  - 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].
  - 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 $|\mathcal{D}| \geq 2$. 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 $D = \{d_1, \ldots, d_l\}$ define $\mathcal{D}' = \langle D, P_1, \ldots, P_l \rangle$ such that $P_i = \{d_i\}$. We write $x = d_i$ instead of $P_i(x)$.

- Translation from CLTL$^\downarrow(D)$ into CLTL($\mathcal{D}'$):
  - $T$ is homomorphic for the Boolean and temporal operators,
  - $T(R(\alpha_1, \ldots, \alpha_n)) = (\bigvee_{R(d_{i_1}, \ldots, d_{i_n})}(\alpha_1 = d_{i_1} \land \cdots \land \alpha_n = d_{i_n}))$,
  - $T(\downarrow x' = \alpha \psi) = \bigwedge_{d_i \in D}(\alpha = d_i) \Rightarrow T(\psi)_{x' = d_i}$, where $T(\psi)_{x' = d_i}$ is obtained from $T(\psi)$ by replacing every occurrence of $x' = d_j$ with $j \neq i$ by $\bot$ and every occurrence of $x' = d_i$ by $\top$.

- The last clause causes an exponential blow up.
Sketch of the proof (II)

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

- Formulae below belong to the flat fragment:

\[
\downarrow x' = x \ F(x' < y) \quad \neg G \downarrow y = x \ XG x \neq y
\]

- $\text{CLTL}(D)$ is in the flat fragment of $\text{CLTL}^\downarrow(D)$.

- Flat $\text{CLTL}^\downarrow(\mathbb{N}, =)$ is strictly more expressive than $\text{CLTL}(\mathbb{N}, =)$. 
Reduction to $\text{CLTL}(\mathcal{D})$

- Translation from flat $\text{CLTL}^{\downarrow}(\mathcal{D})$ into $\text{CLTL}(\mathcal{D})$:
  
  $\begin{align*}
  &\quad \text{T}(c) \overset{\text{def}}{=} c' \text{ where } c' \text{ is obtained from } c \text{ by replacing each rigid variable } y \text{ by } y_{\text{new}}, \\
  &\quad \text{T} \text{ is homomorphimic for Boolean and temporal operators,} \\
  &\quad \text{T}(\downarrow_{y=x^{n}x} \psi) \overset{\text{def}}{=} y_{\text{new}} = X^{n}x \land G(y_{\text{new}} = Xy_{\text{new}}) \land \text{T}(\psi).
  \end{align*}$

- **Lemma.** $\mathcal{D}$ constraint system with equality. For any formula $\phi$ of the flat fragment of $\text{CLTL}^{\downarrow}(\mathcal{D})$, $\phi$ is $\text{CLTL}^{\downarrow}(\mathcal{D})$ satisfiable iff $\text{T}(\phi)$ is $\text{CLTL}(\mathcal{D})$ satisfiable.

- **Corollary.** Flat fragments of $\text{CLTL}^{\downarrow}(\mathbb{Z}, <, =)$, $\text{CLTL}^{\downarrow}(\mathbb{N}, <, =)$, $\text{CLTL}^{\downarrow}(\mathbb{R}, <, =)$, and $\text{CLTL}^{\downarrow}(\mathcal{D})$ with $\mathcal{D}$ finite are $\text{PSPACE}$-complete.
\[ \Sigma^1_1 \text{-completeness of } \mathsf{CLTL}^\downarrow (\mathbb{N}, =) \]

- \( \mathsf{CLTL}^\downarrow (\mathbb{N}, =) \): minimal pure-future constrained version of \( \mathsf{LTL} \) with unrestricted freeze operator.

- Reduction of the rec. problem for nondet. 2-counter machines.

- Instructions of the form

\[
\begin{align*}
  l &: \ C_i := C_i + 1; \text{ goto } l' \text{ or goto } l'' \\
  l &: \ C_i := C_i - 1; \text{ goto } l' \text{ or goto } l'' \\
  l &: \text{ if } C_i = 0 \text{ then goto } l' \text{ else goto } l''
\end{align*}
\]

- \textbf{Theorem.} \( D \) infinite set. Satisfiability for \( \mathsf{CLTL}^\downarrow (D, =) \) restricted to one flexible variable and two rigid variables is \( \Sigma^1_1 \)-hard.
Encoding of configurations

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

\[ ddd' d \ldots d' \ldots f_1^1 \ldots f_{c_1}^1 eee' e'' f_1^2 \ldots f_{c_2}^2 \]

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) \( f_1^i, \ldots, f_{c_i}^i \) are mutually distinct.
Global encoding

\[ \phi_{n}^{glob} \overset{\text{def}}{=} G(\text{start}_d \Rightarrow \psi_n^1 \land \text{start}_e \Rightarrow \psi_n^2) \]

in \( dd'd \ldots d' \ldots \) two consecutive values are distinct

\[ \psi_n^1 \overset{\text{def}}{=} \left( \bigwedge_{i=1}^{n+3} X^i x \neq X^{i+1} x \right) \land \left( \bigwedge_{l=1}^{n} X^2 x = X^{l+3} x \land \bigwedge_{j=1}^{l-1} X^2 x \neq X^{j+3} x \land \bigwedge_{j=l+1}^{n} X^2 x \neq X^{j+3} x \right) \]

in \( \ldots d' \ldots \) exactly one value equals \( d' \)

\[ X^{n+4}(\psi_{\text{dist}} \cup \text{start}_e) \]

\[ f_1^1 \ldots f_{c_1}^1 \text{ mutually distinct} \]

\[ \psi_n^2 \overset{\text{def}}{=} \left( \bigwedge_{i=1}^{3} X^i x \neq X^{i+1} x \right) \land \left( f_1^2 \ldots f_{c_2}^2 \text{ mutually distinct} \right) \]

\[ X^4(\psi_{\text{dist}} \cup \text{start}_d) \]

On the freeze operator in constraint LTL – p. 25
More formulae

- \( \psi^{\text{dist}} \overset{\text{def}}{=} \neg \text{start}_{d\vee e} \land \downarrow y=x \ X ((\neg \text{start}_{d\vee e} \land x \neq y) \mathbf{U} \text{start}_{d\vee e}). \)

- \( l : \ C_2 := C_2 - 1; \ \text{goto} \ l' \ \text{or goto} \ l''. \)

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

- You do not want to see \( \chi_{eq}^1 \) and \( \chi_{dec}^2 \)!!
Corollaries

- **Corollary.** RHLTL with temporal operators $U$ and $X$ and without propositional variables is $\Sigma_1^1$-complete.

- **Corollary.** TPTL without monotonicity is $\Sigma_1^1$-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.