Decidability and complexity issues for subclasses of counter systems

Lecture 5
LTL for admissible CS + Exercises

Stéphane Demri
demri@lsv.ens-cachan.fr
LSV, ENS Cachan, CNRS, INRIA

Course 2.9 – MPRI – 2010/2011
“Verification of parametrized and dynamic systems”
Plan of the lecture

- Previous lecture: Flat affine counter systems with finite monoid property.
- One-hour course on model-checking Presburger LTL by translation into Presburger arithmetic.
- Exercises.
Specifying existence of runs in temporal logic

- Repeated reachability can be obviously expressed by $\mathbb{G} \mathbb{F} q_f$.

- Initialized VASS $(\mathcal{V}, (q, \vec{z}))$ is unbounded iff there is a run $(q, \vec{z}) \xrightarrow{*} (q', \vec{y}) \xrightarrow{*} (q', \vec{y}')$ with $\vec{y} \prec \vec{y}'$ for some $q'$.

- In temporal logic lingua:

$$\mathcal{V}, (q, \vec{z})) \models \mathbb{E} \exists y_1, \ldots, y_n \mathbb{F} \left( \bigwedge_{i=1}^{n} x_i = y_i \land \mathbb{F} \left( \bigwedge_{i=1}^{n} x_i \geq y_i \land \bigvee_{i=1}^{n} x_i > y_i \right) \right)$$

- Linear-time temporal logics offer genericity and fragments can be easily designed.
LTL syntax (standard)

- LTL formulae:

\[ \varphi, \psi ::= p \mid \neg \varphi \mid \varphi \land \psi \mid \varphi \lor \psi \mid X \varphi \mid \varphi U \psi \]

- Atomic formulae are propositional variables.

- Later, control states or arithmetical constraints about counter values are considered at the atomic level.

- LTL models \( \rho \) are \( \omega \)-sequences of propositional valuations of the form \( \rho : \mathbb{N} \rightarrow \mathcal{P}(PROP) \).
“always” and “until” (quick reminder)

- The operator $G$ is the dual of $F$: whatever the formula $\varphi$ may be, if $\varphi$ is always satisfied, then it is not true that $\neg \varphi$ will some day be satisfied, and conversely. ($G\varphi$ and $\neg F \neg \varphi$ are equivalent.)

\[ Gp: \text{ always } p \]

- The $\cup$ operator is richer and more complicated than the combinator $F$. $\varphi_1 \cup \varphi_2$ states that $\varphi_1$ is true until $\varphi_2$ is true.

\[ p \cup q: p \text{ until } q \]

$G(\text{alert } \Rightarrow F \text{ halt})$ can be refined with

\[ G(\text{alert } \Rightarrow (\text{alarm } \cup \text{ halt})). \]
Satisfaction relation (formal semantics)

- $\rho, i \models p \iff p \in \rho(i)$,
- $\rho, i \models \neg \varphi \iff \rho, i \not\models \varphi$,
- $\rho, i \models \varphi_1 \land \varphi_2 \iff \rho, i \models \varphi_1$ and $\rho, i \models \varphi_2$,
- $\rho, i \models x \varphi \iff \rho, i + 1 \models \varphi$,
- $\rho, i \models \varphi_1 \cup \varphi_2 \iff$ there is $j \geq i$ such that $\rho, j \models \varphi_2$ and $\rho, k \models \varphi_1$ for all $i \leq k < j$.

$F \varphi \overset{\text{def}}{=} \top \lor \varphi$, $G \varphi \overset{\text{def}}{=} \neg F \neg \varphi$, $\varphi \Rightarrow \psi \overset{\text{def}}{=} \neg \varphi \lor \psi$, etc.
About LTL

- Models(φ): set of models ρ such that ρ, 0 ⊨ φ.

- Models can be viewed as ω-words over the alphabet \( \mathcal{P}(PROP) \).

- Models(φ) can be effectively represented by a Büchi automaton \( A_\varphi \).

- Satisfiability and model-checking (see later) are \( \text{PSPACE} \)-complete problems [Sistla & Clarke, JACM 85].
New ingredients

• Enriched models of the form \((q_0, \vec{x}_0), (q_1, \vec{x}_1), \ldots\).

• Control states \(q\) as atomic formulae.

• Arithmetical constraints about counter values, e.g. \((x_1 > x_2)\).

• Comparing values at successive positions, e.g. \(x_1 \geq x_2\).

• First-order quantification over counter values, e.g. \(\exists y \ G(x_1 \leq y) \approx \text{"Along the run, counter 1 is bounded."}\).
**LTL\textsuperscript{CS}(PrA) syntax**

- Queen logic LTL\textsuperscript{CS}(PrA) (fragments are defined from it).

- Giving up the standard abstraction: propositional variables understood as properties about the current configuration.

- $\text{VAR}^p = \{y_1, y_2, \ldots\}$: set of integer variables.

- $\text{VAR} = \{x_1, x_2, \ldots\}$: set of counter variables.

- $\mathcal{Q} = \{q_1, q_2, \ldots\}$: set of control state symbols.

- LTL\textsuperscript{CS}(PrA) formulae:

  $\varphi ::= \psi \mid q \mid \varphi \land \varphi \mid \neg \varphi \mid X\varphi \mid \varphi \lor \varphi \mid \exists y \varphi$

- $\psi$ is a Presburger formula with free variables included in $\text{VAR}^p \cup \text{VAR}$,

- $q \in \mathcal{Q}$. 
Examples

- Along the run, infinitely often counter 1 is equal to counter 2:
  \[ G F (x_1 = x_2) \]

- Along the run, counter 1 is bounded:
  \[ \exists y G(x_1 \leq y) \]

- Counter 1 never takes twice the same value:
  \[ G(\exists y (y = x_1) \land XG(y \neq x_1)) \]

- Never, counter 1 is incremented:
  \[ G(\exists y y = x_1 \land X(y + 1 \neq x_1)) \]
Satisfaction relation

- Model \( \rho \) of dimension \( n \): element of \( (Q \times \mathbb{N}^n)^\omega \).
  \( \rho = (q_0, \vec{x}_0), (q_1, \vec{x}_1), \ldots \).

- Environment \( \mathcal{E} \): partial map \( \text{VAR}^p \rightarrow \mathbb{N} \).

- \( \rho, i \models \mathcal{E} q \overset{\text{def}}{\iff} q = q_i \).

- \( \rho, i \models \mathcal{E} \psi \overset{\text{def}}{\iff} \mathbf{v}_i \models \psi \) in \( \text{PrA} \) with \( \mathbf{v}_i \) extends \( \mathcal{E} \) s.t. \( \mathbf{v}_i(x_j) = \vec{x}_i(j) \) (\( j \in [1, n] \)), assuming \( \psi \) is a Presburger formula with free variables in \( \text{VAR}^p \cup \{x_1, \ldots, x_n\} \).

- \( \rho, i \models \mathcal{E} x \varphi \overset{\text{def}}{\iff} \rho, i + 1 \models \mathcal{E} \varphi \).

- \( \rho, i \models \mathcal{E} \exists y \varphi \) iff there is \( k \in \mathbb{N} \) such that \( \rho, i \models \mathcal{E}[y \mapsto k] \varphi \).
Decision problems for $\text{LTL}^{\text{CS}}(\text{PrA})$

- Semi-closed formula: no variable from $\text{VAR}^p$ is free. $F(x_1 = y)$ is not semi-closed unlike $G(x_1 > x_2)$ and $\exists y \ G(x_1 \leq y)$.

- **Existential Model-Checking Problem**

  **Input:** CS $S = (Q, n, \delta)$, $(q_0, \vec{x}_0)$ and semi-closed formula $\varphi$ with free variables in $\{x_1, \ldots, x_n\}$.

  **Question:** Is there an infinite run $\rho$ starting at $(q_0, \vec{x}_0)$ such that $\rho, 0 \models_\varnothing \varphi$?

  (Infinite runs of CS are $\text{LTL}^{\text{CS}}(\text{PrA})$ models)
A simple reduction

- The control state repeated reachability problem can be reduced to the model-checking problem for $\text{LTL}^{CS}(\text{PrA})$.

- Let $\mathcal{S}$, $(q, \vec{x})$ and $q_f$ be an instance.

- Equivalence:
  - there is an infinite run from $(q, \vec{x})$ such that $q_f$ is repeated infinitely often,
  - there is an infinite run $\rho$ from $(q, \vec{x})$ such that $\rho, 0 \models G F q_f$.

- This can be extended to the sequence $F_1, \ldots, F_N$ understood conjunctively and each $F_i$ disjunctively.

$$\bigwedge_{i=1}^{N} \left( \bigvee_{q' \in F_i} G F q' \right)$$
Temporal logics with Presburger constraints

- Constraints on the number of event occurrences.
  [Bouajjani et al., LICS’95; Laroussinie et al., TIME’10]

- Constraints on XML documents.
  [Dal Zilio & Lugiez, RTA’03; Seidl et al., ICALP’04]

- LTL with first-order variables for log auditing.
  [Roger & Goubault-Larrecq, CSFW’01]

- Temporal semantics of imperative programs.
  [Manna & Pnueli, 1992]
  Program variable $x$ never decreases below its initial value:
  $$\exists y \ (x = y) \land G(x \geq y)$$

- and many many others . . .
Decidable model-checking problem

- Model-checking restricted to $\text{LTL}(Q)$ is already undecidable ...

- $\text{LTL}^{\text{CS}}(\text{PrA})$ formulae:
  
  $$\varphi ::= \psi \mid q \mid \varphi \land \varphi \mid \neg \varphi \mid X\varphi \mid \varphi U \varphi \mid \exists y \varphi$$

- **Theorem**: Existential model-checking problem for $\text{LTL}^{\text{CS}}(\text{PrA})$ restricted to admissible counter systems is decidable.

- The proof partly uses that the reachability relation for admissible counter systems is effectively semilinear ...

- ...but this is not sufficient to show the result.
Properties for admissible counter systems (reminder)

• When \( t_1 \cdots t_N \) is a sequence of consecutive transitions from \( q \) to \( q' \), there is \( \chi(\vec{x}, \vec{x'}) \) such that for every \( v \), we have \( v \models \chi \iff (q, (v(x_1), \ldots, v(x_n))) \xrightarrow{t_1 \cdots t_N} (q', (v(x'_1), \ldots, v(x'_n))) \)

• When \( q = q' \) above (loop), there is \( \chi'(\vec{x}, z, \vec{x'}) \) such that for every \( v \), we have \( v \models \chi' \iff (q, (v(x_1), \ldots, v(x_n))) \xrightarrow{(t_1 \cdots t_N)^v(z)} (q, (v(x'_1), \ldots, v(x'_n))) \)

\( (\text{REL}(\chi(\vec{x}, \vec{x'}))) \) has a Presburger counting iteration)
Proof – Showing a stronger property

• Instance: admissible CS \( S = (Q, n, \delta), (q, \bar{x}), \varphi \).

• W.l.o.g., \( \varphi \) has no control states as atomic formulae.

• We wish to check whether there is an infinite run \( \rho \) from \((q, \bar{x})\) such that \( \rho, 0 \models \varphi \).

• We build \( \psi \) such that for every \( \mathbf{v} \), propositions below are equivalent:
  1. \( \mathbf{v} \models \psi \).
  2. \( \exists \) an infinite run \( \rho \) from \((q, (\mathbf{v}(x_1), \ldots, \mathbf{v}(x_n)))\) s.t. \( \rho, 0 \models \varphi \).

• It remains to test the satisfaction of \( \psi \land (\bigwedge_{i \in [1, n]} x_i = \bar{x}(i)) \).
Proof – Run schemata

- Run schemata:
  \[ t_1 t_3 (t_4 t_2 t_3)^* t_5 t_6^\omega, t_1 t_3 (t_4 t_2 t_3)^\omega, t_7 t_8 (t_10 t_9)^* t_11 t_6^\omega, t_7 t_8 (t_10 t_9)^\omega. \]

- Number of run schemata is at most exponential in the size of \( S \).

- The run schemata can be effectively computed.
Quantifying over runs with natural numbers

• From $L = u_1(v_1)^* u_2(v_2)^* \cdots (v_k)^\omega$ and $m_1, \ldots, m_{k-1} \in \mathbb{N}$, we get the sequence

$$u_1(v_1)^{m_1} u_2(v_2)^{m_2} \cdots (v_k)^\omega$$

• The sequence may correspond to an infinite run from $(q, \vec{x})$ (but not necessarily).

• With $L$ and $m_1, \ldots, m_{k-1}$, there is at most one infinite run from $(q, \vec{x})$ respecting $u_1(v_1)^{m_1} u_2(v_2)^{m_2} \cdots (v_k)^\omega$.

• Indeed, update functions in affine CS are deterministic.
Proof – Auxiliary formulae

• Auxiliary Presburger formulae such that for every \( \mathbf{v} \),
  
  • \( \mathbf{v} \models \chi_L(\exists z_1, \ldots, z_{k-1}, \vec{x}) \) iff there is an infinite run from
    \( (q, (\mathbf{v}(x_1), \ldots, \mathbf{v}(x_n))) \) resp. \( u_1(v_1)^{v(z_1)}u_2(v_2)^{v(z_2)}\ldots(v_k)^{\omega} \).

  • \( \mathbf{v} \models \chi_L^{\text{steps}}(z_1, \ldots, z_{k-1}, \vec{x}, z, \vec{x'}) \) iff \( \mathbf{v} \models \chi_L(\exists z_1, \ldots, z_{k-1}, \vec{x}) \)
    and the \( \mathbf{v}(z) \)th tuple of counter values is \( (\mathbf{v}(x_1'), \ldots, \mathbf{v}(x_n')) \).

• \( \psi \) defined as a disjunction:

\[
\bigvee_{L=u_1(v_1)^*u_2(v_2)^*_\ldots(v_k)^{\omega}} (\exists z_1, \ldots, z_{k-1}, z_0 \chi_L(\exists z_1, \ldots, z_{k-1}, \vec{x})^* \\
\bigwedge z_0 = 0 \land t_L(z_0, \varphi))
\]
From FO-definable temporal operators to FO on \((\mathbb{N}, +)\)

- \(t_L\) is homomorphic for Boolean connectives.
- \(t_L(z, x\psi) \equiv \exists z' (z' = z + 1) \land t_L(z', \psi)\).
- The definition of \(t_L(z, \psi_1 \cup \psi_2)\) is analogous.
- \(t_L(z, \forall y \psi) \equiv \forall y t_L(z, \psi)\).
- \(t_L(z, \psi(y, x)) \equiv \forall x' (\chi_{L_{\text{steps}}}^{\text{steps}}(z_1, \ldots, z_{k-1}, \bar{x}, z, x') \Rightarrow \psi(y, x'))\)
where \(\psi(y, x)\) is an atomic formula with a tuple \(\bar{y}\) of variables from \(\text{VAR}^p\).
Almost admissible counter system $S_u$

$x'_1 = x_1 + 1 \quad x'_2 = x_2 + 1 \quad x'_3 = x_3 + 1$

- $S_u$ is an affine counter system.
- At most one transition between two control states.
- ...but $S_u$ is not flat!
Undecidability

- **Proposition:** Model-checking problem for $\text{LTL}^\text{CS}(\text{PrA})$ restricted to the affine counter system $S_u$ is undecidable.

- Proof by reduction from the recurrence problem for nondeterministic Minsky machines that is shown $\Sigma_1^1$-hard in [Alur & Henzinger, JACM 94].

- Two types of instructions (with nondeterminism)
  
  1 : $C_i := C_i + 1$; goto $l'$ or goto $l''$.

  1 : if $C_i = 0$ then goto $l'$ else $C_i := C_i - 1$; goto $l''_0$ or goto $l''_1$.

- Recurrence problem checks the existence of an infinite run in which instruction 1 is repeated infinitely often.
We represent the configurations of machine $M$ with $N$ instructions by triples $(c_1, c_2, l)$ where $1 \leq l \leq N$, $c_1, c_2 \in \mathbb{N} \geq 0$.

$M$ visits 1 infinitely often iff there is an infinite run $\rho$ starting at $(q_2, (0, 0, 1))$ such that $\rho, 0 \models \varphi$.

Formula $\varphi$:

$$GF(x_3 = 1 \land xq_0) \land \bigwedge_{1 \leq l \leq N} G\psi_l,$$

where $\psi_l$ encodes the $l$-th instruction.
Relating successive configurations

- $l$th instruction “$C_1 := C_1 + 1; \text{goto } l''_0 \text{ or goto } l''_1$” is encoded by

$$\forall y, z \ (x_1 = y \land x_2 = z \land x_3 = l \land xq_0) \Rightarrow x(\neg(xq_0) \cup (xq_0 \land x_1 = y + 1 \land x_2 = z \land (x_3 = l''_0 \lor x_3 = l''_1))).$$

- Other instructions can be encoded similarly.

$$x'_1 = x_1 + 1 \quad x'_2 = x_2 + 1 \quad x'_3 = x_3 + 1$$

$x'_1 = x'_2 = x'_3 = 0$
Exo. 1

• Let $LTL^+$ be the fragment of the logic $LTL^{CS}(PrA)$
  • with temporal operators $x$, $u$ and standard Boolean connectives,
  • atomic formulae are restricted to control states or zero-tests of the form $x_j = 0$.
  • without first-order quantification.

• Existential model-checking problem for $LTL^+$ restricted to VASS:
  input: VASS $\mathcal{V}$, configuration $(q, \vec{x})$ and a formula $\varphi$ built over the control states and counters from $\mathcal{V}$.
  question: is there an infinite run starting at $(q, \vec{x})$ satisfying $\varphi$?
Exo. 1

For each formula below, determine whether there is an infinite run starting at \((A, \vec{0})\) such that \(\rho, 0 \models \varphi\).

1. (a) \(\varphi = GF A\); (b) \(\varphi = GF (x_2 = 0)\),
   
   (c) \(\varphi = GF (x_1 = 0) \land GF C\); (d) \(\varphi = G(C \Rightarrow XG \neg(x_1 = 0))\),
   
   (e) \((GF A) \land (GF B) \land (GF C) \land (GF x_2 = 0) \land (GF \neg(x_1 = 0))\).

2. What are the formulae among (a)-(e) such that all the infinite runs starting at \((A, \vec{0})\), we have \(\rho, 0 \models \varphi\)?

3. Show that the existential model-checking for LTL\(^+\) restricted to VASS is undecidable.
Exo. 2

• In this exercise, we shall make use of the fundamental result that the reachability problem for VASS is decidable. So, we assume that we have a terminating procedure such that given a VASS $\mathcal{V}$, and two configurations $(q, \vec{x})$ and $(q', \vec{x}')$, returns 'yes' iff there is a run from $(q, \vec{x})$ to $(q', \vec{x}')$ respecting the transitions from $\mathcal{V}$.

• Let us consider a first model that extends VASS by allowing transitions of the form

$$t = q \xrightarrow{\vec{b}} q'$$

with $\vec{b} \in \mathbb{N}^n$ such that $(q, \vec{a}) \xrightarrow{t} (q', \vec{a}')$ iff $\vec{b} \leq \vec{a}$ and $\vec{a} = \vec{a}'$. As usual, $\vec{b} \leq \vec{a}$ $\overset{\text{def}}{\iff}$ for $i \in [1, n]$, we have $b(i) \leq a(i)$. Show that the covering problem for this extended class of VASS can be solved in exponential space.
Exo. 2

• Let us consider another model that extends VASS by allowing transitions of the form

\[ t = q \xrightarrow{x_i \leq k} q' \quad \text{with } i \in [1, n], \ k \in \mathbb{N} \]

such that \((q, \vec{a}) \xrightarrow{t} (q', \vec{a}')\) iff \(\vec{a}(i) \leq k\) and \(\vec{a} = \vec{a}'\). Show that the covering problem for this extended class of VASS is undecidable.

• Let us consider a third model that extends VASS by allowing transitions of the form

\[ t = q \xleftarrow{\vec{b}} q' \quad \text{with } \vec{b} \in \mathbb{N}^n \]

such that \((q, \vec{a}) \xleftarrow{t} (q', \vec{a}')\) iff \(\vec{a} \preceq \vec{b}\) and \(\vec{a} = \vec{a}'\). Define a polynomial-time reduction from the reachability problem for VASS into the covering problem for this extended class of VASS. Comment this result.
Exo. 2

• Let $\mathcal{V}$ be an extended VASS of dimension $n$ (with set of locations $Q$) such that the extended transitions are exactly

$$q_1 \xrightarrow{\vec{b}_1} q'_1, \ldots, q_N \xrightarrow{\vec{b}_N} q'_N$$

with $\vec{b}_1, \ldots, \vec{b}_N \in \mathbb{N}^n$. Show that if there is a run from $(q, \vec{x})$ to $(q', \vec{x}')$, then there is a run such that the number of times extended transitions are fired is at most exponential in the size of $\mathcal{V}$. Provide a precise bound.

• Given an initial configuration $(q, \vec{x})$, design an algorithm that computes the set below:

$$\{(q_i, \vec{a}) \in Q \times \mathbb{N}^n : i \in [1, N], \vec{a} \preceq \vec{b}_i, (q, \vec{x}) \xrightarrow{*} (q_i, \vec{a}) \text{ in } \mathcal{V}\}$$

• Conclude that the reachability problem and the covering problem for this extended class of VASS are decidable.