

# 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  $G F q_f$ .
- 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:

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

- Linear-time temporal logics offer genericity and fragments can be easily designed.

# LTL syntax (standard)

- LTL formulae:

$$\varphi, \psi ::= p \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid X\varphi \mid \varphi U \psi$$

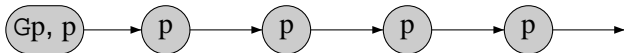
- Atomic formulae are propositional variables.
- Later, control states or arithmetical constraints about counter values are considered at the atomic level.
- LTL models  $\rho$  are  $\omega$ -sequences of propositional valuations of the form  $\rho : \mathbb{N} \rightarrow \mathcal{P}(\text{PROP})$ .

## “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.)

$Gp$ : always  $p$



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

$pUq$ :  $p$  until  $q$



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

$G(\text{alert} \Rightarrow (\text{alarm} U \text{halt}))$ .

## Satisfaction relation (formal semantics)

- $\rho, i \models p \stackrel{\text{def}}{\Leftrightarrow} p \in \rho(i),$
- $\rho, i \models \neg\varphi \stackrel{\text{def}}{\Leftrightarrow} \rho, i \not\models \varphi,$
- $\rho, i \models \varphi_1 \wedge \varphi_2 \stackrel{\text{def}}{\Leftrightarrow} \rho, i \models \varphi_1 \text{ and } \rho, i \models \varphi_2,$
- $\rho, i \models X\varphi \stackrel{\text{def}}{\Leftrightarrow} \rho, i + 1 \models \varphi,$
- $\rho, i \models \varphi_1 U \varphi_2 \stackrel{\text{def}}{\Leftrightarrow} \text{there is } j \geq i \text{ such that } \rho, j \models \varphi_2 \text{ and } \rho, k \models \varphi_1 \text{ for all } i \leq k < j.$

$F\varphi \stackrel{\text{def}}{=} \top U \varphi, G\varphi \stackrel{\text{def}}{=} \neg F \neg \varphi, \varphi \Rightarrow \psi \stackrel{\text{def}}{=} \neg \varphi \vee \psi, \text{ etc.}$

# About LTL

- $\text{Models}(\varphi)$ : set of models  $\rho$  such that  $\rho, 0 \models \varphi$ .
- Models can be viewed as  $\omega$ -words over the alphabet  $\mathcal{P}(\text{PROP})$ .
- $\text{Models}(\varphi)$  can be effectively represented by a Büchi automaton  $\mathcal{A}_\varphi$ .
- Satisfiability and model-checking (see later) are PSPACE-complete problems [Sistla & Clarke, JACM 85].

## New ingredients

- Enriched models of the form  $(q_0, \vec{x}_0), (q_1, \vec{x}_1), \dots$
- Control states  $q$  as atomic formulae.
- Arithmetical constraints about counter values, e.g.  $(x_1 > x_2)$ .
- Comparing values at successive positions, e.g.  $x_1 > \mathbf{X}x_2$ .
- First-order quantification over counter values, e.g.  
 $\exists y G(x_1 \leq y)$ .  $\approx$  “Along the run, counter 1 is bounded.”

# LTL<sup>CS</sup>(PrA) syntax

- Queen logic LTL<sup>CS</sup>(PrA) (fragments are defined from it).
- Giving up the standard abstraction: propositional variables understood as properties about the current configuration.
- $\text{VAR}^p = \{y_1, y_2, \dots\}$ : set of integer variables.
- $\text{VAR} = \{x_1, x_2, \dots\}$ : set of counter variables.
- $\mathcal{Q} = \{q_1, q_2, \dots\}$ : set of control state symbols.
- LTL<sup>CS</sup>(PrA) formulae:

$$\varphi ::= \psi \mid \mathbf{q} \mid \varphi \wedge \varphi \mid \neg \varphi \mid \mathbf{x}\varphi \mid \varphi \cup \varphi \mid \exists \mathbf{y} \varphi$$

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

## 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:

$$G(\exists y (y = x_1) \wedge \neg G(y \neq x_1))$$

- Never, counter 1 is incremented:

$$G(\exists y y = x_1 \wedge \neg X(y + 1 \neq x_1))$$

## Satisfaction relation

- Model  $\rho$  of dimension  $n$ : element of  $(\mathcal{Q} \times \mathbb{N}^n)^\omega$ .  
 $\rho = (q_0, \vec{x}_0), (q_1, \vec{x}_1), \dots$
- Environment  $\mathcal{E}$ : partial map  $\text{VAR}^p \rightarrow \mathbb{N}$ .
- $\rho, i \models_{\mathcal{E}} q \stackrel{\text{def}}{\iff} q = q_i$ .
- $\rho, i \models_{\mathcal{E}} \psi \stackrel{\text{def}}{\iff} \mathbf{v}_i \models \psi$  in 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  
 $\text{VAR}^p \cup \{x_1, \dots, x_n\}$ .
- $\rho, i \models_{\mathcal{E}} X\varphi \stackrel{\text{def}}{\iff} \rho, i + 1 \models_{\mathcal{E}} \varphi$ .
- $\rho, i \models_{\mathcal{E}} \exists y \varphi$  iff there is  $k \in \mathbb{N}$  such that  $\rho, i \models_{\mathcal{E}[y \mapsto k]} \varphi$ .

## Decision problems for $LTL^{CS}(\text{PrA})$

- Semi-closed formula: no variable from  $\text{VAR}^P$  is free.  
 $\mathbb{F}(x_1 = y)$  is not semi-closed unlike  $G(x_1 > x_2)$  and  $\exists y G(x_1 \leq y)$ .
- EXISTENTIAL MODEL-CHECKING PROBLEM  
**Input:** CS  $\mathcal{S} = (Q, n, \delta)$ ,  $(q_0, \vec{x}_0)$  and semi-closed formula  $\varphi$  with free variables in  $\{x_1, \dots, x_n\}$ .  
**Question:** Is there an infinite run  $\rho$  starting at  $(q_0, \vec{x}_0)$  such that  $\rho, 0 \models_{\emptyset} \varphi$ ?

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

## A simple reduction

- The control state repeated reachability problem can be reduced to the model-checking problem for  $LTL^{CS}(\text{PrA})$ .
- 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  $F_1, \dots, F_N$  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:

$$\exists y (x = y) \wedge G(x \geq y)$$

- and many many others . . .

# Decidable model-checking problem

- Model-checking restricted to  $LTL(Q)$  is already undecidable  
...

- $LTL^{CS}(PrA)$  formulae:

$$\varphi ::= \psi \mid \mathbf{q} \mid \varphi \wedge \varphi \mid \neg \varphi \mid \mathbf{x}\varphi \mid \varphi \mathbf{U} \varphi \mid \exists \mathbf{y} \varphi$$

- **Theorem:** Existential model-checking problem for  $LTL^{CS}(PrA)$  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  $\mathbf{v}$ , we have  $\mathbf{v} \models \chi$  iff

$$(q, (\mathbf{v}(x_1), \dots, \mathbf{v}(x_n))) \xrightarrow{t_1 \cdots t_N} (q', (\mathbf{v}(x'_1), \dots, \mathbf{v}(x'_n)))$$

- When  $q = q'$  above (loop), there is  $\chi'(\vec{x}, z, \vec{x}')$  such that for every  $\mathbf{v}$ , we have  $\mathbf{v} \models \chi'$  iff

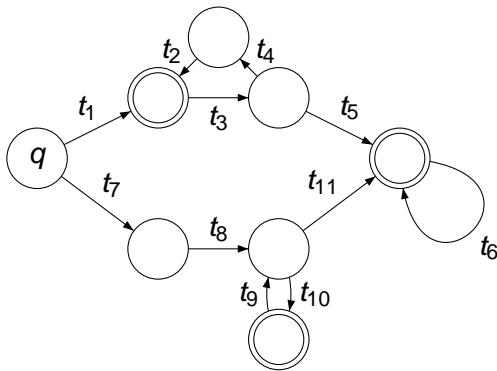
$$(q, (\mathbf{v}(x_1), \dots, \mathbf{v}(x_n))) \xrightarrow{(t_1 \cdots t_N)^{\mathbf{v}(z)}} (q, (\mathbf{v}(x'_1), \dots, \mathbf{v}(x'_n)))$$

(REL( $\chi(\vec{x}, \vec{x}')$ )) has a Presburger counting iteration)

## Proof – Showing a stronger property

- Instance: admissible CS  $\mathcal{S} = (Q, n, \delta), (q, \vec{x}), \varphi$ .
- W.l.o.g.,  $\varphi$  has no control states as atomic formulae.
- We wish to check whether there is an infinite run  $\rho$  from  $(q, \vec{x})$  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  $(q, (\mathbf{v}(x_1), \dots, \mathbf{v}(x_n)))$  s.t.  $\rho, 0 \models \varphi$ .
- It remains to test the satisfaction of  $\psi \wedge (\bigwedge_{i \in [1, n]} x_i = \vec{x}(i))$ .

## 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  $\mathcal{S}$ .
- 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  $m_1, \dots, m_{k-1} \in \mathbb{N}$ , 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  $m_1, \dots, m_{k-1}$ , 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

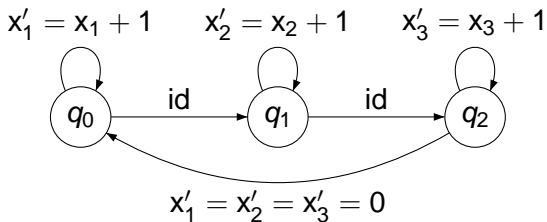
- Auxiliary Presburger formulae such that for every  $\mathbf{v}$ ,
  - $\mathbf{v} \models \chi_L^{\exists}(z_1, \dots, z_{k-1}, \vec{x})$  iff there is an infinite run from  $(q, (\mathbf{v}(x_1), \dots, \mathbf{v}(x_n)))$  resp.  $u_1(v_1)^{\mathbf{v}(z_1)} u_2(v_2)^{\mathbf{v}(z_2)} \dots (v_k)^{\omega}$ .
  - $\mathbf{v} \models \chi_L^{\text{steps}}(z_1, \dots, z_{k-1}, \vec{x}, z, \vec{x}')$  iff  $\mathbf{v} \models \chi_L^{\exists}(z_1, \dots, z_{k-1}, \vec{x})$  and the  $\mathbf{v}(z)$ th tuple of counter values is  $(\mathbf{v}(x'_1), \dots, \mathbf{v}(x'_n))$ .
- $\psi$  defined as a disjunction:

$$\bigvee_{L=u_1(v_1)^* u_2(v_2)^* \dots (v_k)^{\omega}} (\exists z_1, \dots, z_{k-1}, z_0 \chi_L^{\exists}(z_1, \dots, z_{k-1}, \vec{x}) \wedge z_0 = 0 \wedge \mathfrak{t}_L(z_0, \varphi))$$

# From FO-definable temporal operators to FO on $(\mathbb{N}, +)$

- $t_L$  is homomorphic for Boolean connectives.
- $t_L(z, X\psi) \stackrel{\text{def}}{=} \exists z' (z' = z + 1) \wedge t_L(z', \psi)$ .
- The definition of  $t_L(z, \psi_1 \cup \psi_2)$  is analogous.
- $t_L(z, \forall y \psi) \stackrel{\text{def}}{=} \forall y t_L(z, \psi)$ .
- $t_L(z, \psi(\vec{y}, \vec{x})) \stackrel{\text{def}}{=} \forall \vec{x}' (\chi_L^{\text{steps}}(z_1, \dots, z_{k-1}, \vec{x}, z, \vec{x}') \Rightarrow \psi(\vec{y}, \vec{x}'))$   
where  $\psi(\vec{y}, \vec{x})$  is an atomic formula with a tuple  $\vec{y}$  of variables from  $\text{VAR}^p$ .

## Almost admissible counter system $\mathcal{S}_U$



- $\mathcal{S}_U$  is an affine counter system.
- At most one transition between two control states.
- ... but  $\mathcal{S}_U$  is not flat !

# Undecidability

- **Proposition:** Model-checking problem for  $LTL^{CS}(\text{PrA})$  restricted to the affine counter system  $\mathcal{S}_U$  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)
  - $I : C_i := C_i + 1; \text{ goto } l' \text{ or } \text{ goto } l''.$
  - $I : \text{ if } C_i = 0 \text{ then } \text{ goto } l' \text{ else } C_i := C_i - 1; \text{ goto } l'_0 \text{ or } \text{ goto } l'_1.$
- Recurrence problem checks the existence of an infinite run in which instruction 1 is repeated infinitely often.

## Formula $\varphi$

- 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  $\varphi$ :

$$\text{GF}(x_3 = 1 \wedge \text{x}q_0) \wedge \bigwedge_{1 \leq l \leq N} \text{G}\psi_l,$$

where  $\psi_l$  encodes the  $l$ -th instruction.

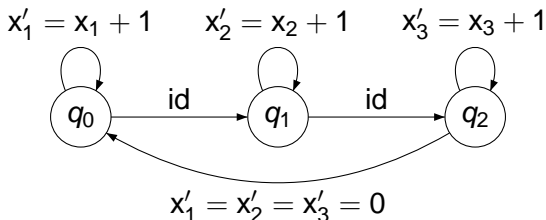
## Relating successive configurations

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

$$\forall y, z (x_1 = y \wedge x_2 = z \wedge x_3 = l \wedge xq_0) \Rightarrow$$

$$x(\underbrace{\neg(xq_0)}_{\text{increase } C_1} \cup (xq_0 \wedge x_1 = y + 1 \wedge x_2 = z \wedge (x_3 = l''_0 \vee x_3 = l''_1))).$$

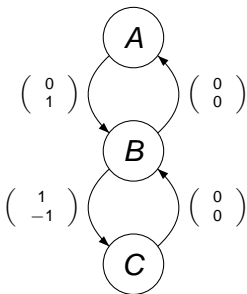
- Other instructions can be encoded similarly.



## 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



- 1 For each formula below, determine whether there is an infinite run starting at  $(A, \vec{0})$  such that  $\rho, 0 \models \varphi$ .
  - (a)  $\varphi = \text{GF } A$ ; (b)  $\varphi = \text{GF } (x_2 = 0)$ ,
  - (c)  $\varphi = \text{GF } (x_1 = 0) \wedge \text{GF } C$ ; (d)  $\varphi = \text{G}(C \Rightarrow \text{XG}\neg(x_1 = 0))$ ,
  - (e)  $(\text{GF } A) \wedge (\text{GF } B) \wedge (\text{GF } C) \wedge (\text{GF } x_2 = 0) \wedge (\text{GF } \neg(x_1 = 0))$ .
- 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  $\text{LTL}^+$  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

$$t = q \xrightarrow{\geq \vec{b}} q' \quad \text{with } \vec{b} \in \mathbb{N}^n$$

such that  $(q, \vec{a}) \xrightarrow{t} (q', \vec{a}')$  iff  $\vec{b} \preceq \vec{a}$  and  $\vec{a} = \vec{a}'$ . As usual,  $\vec{b} \preceq \vec{a} \stackrel{\text{def}}{\iff}$  for  $i \in [1, n]$ , we have  $\vec{b}(i) \leq \vec{a}(i)$ . 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

$$t = q \xrightarrow{\leq \vec{b}} q' \quad \text{with } \vec{b} \in \mathbb{N}^n$$

such that  $(q, \vec{a}) \xrightarrow{t} (q', \vec{a}')$  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

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

with  $\vec{b}_1, \dots, \vec{b}_N \in \mathbb{N}^n$ . 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.