

# Decidable Problems for Counter Systems

Day 5

## Model-Checking Counter Systems

Stéphane Demri

demri@lsv.ens-cachan.fr

LSV, ENS Cachan, CNRS, INRIA

ESSLLI 2010, Copenhagen, August 2010

# Plan of the talk

- Previous lectures:
  - CS, Presburger arithmetic, linear-time temporal logics.
  - VASS, reversal-bounded CA.
- Repeated reachability problem.
- Plain LTL for several classes of counter systems.  
**(Automata)**
- Introduction to admissible counter systems.
- Reachability relation is effectively semilinear.
- $LTL^{CS}(\text{PrA})$  for admissible counter systems.  
**(Presburger Arithmetic)**

## **LTL and Control State Repeated Reachability**

## LTL(Q)

- LTL(Q): fragment where atomic formulae are control states. Example:  $G(q_1 \Rightarrow X q_2)$ .
- LTL(Q) does not speak about counter values but counter values constrain the runs.
- EXISTENTIAL MODEL-CHECKING PROBLEM FOR LTL(Q):
  - Input:** CS  $\mathcal{S} = (Q, n, \delta)$ ,  $(q_0, \vec{x}_0)$  and  $\varphi \in \text{LTL}(Q)$ .
  - Question:** Is there an infinite run  $\rho$  from  $(q_0, \vec{x}_0)$  s.t.  
 $\rho, 0 \models \varphi$ ?
- In this part, we present a sufficient condition for deciding the model-checking problem for LTL(Q) restricted to subclasses of counter systems.
- Problem restricted to CA is already undecidable.

## Projection on runs

- Counter system  $\mathcal{S}$ , configuration  $(q_0, \vec{x}_0)$  and  $\varphi$  in  $\text{LTL}(Q)$ .
- $\rho, 0 \models \varphi$  implies  $\text{proj}_Q(\rho), 0 \models \varphi$ , where  $\text{proj}_Q(\rho) \in Q^\omega$  is obtained from  $\rho$  by erasing the counter values.
- One can effectively construct a Büchi automaton  $\mathcal{A}_\varphi$  over  $Q$  such that:
  - $L(\mathcal{A}_\varphi)$  is the set of models of  $\varphi$ .
  - Size of  $\mathcal{A}_\varphi$  is at most exponential in size of  $\varphi$ .(see Day 2 slides)
- In  $\mathcal{A}_\varphi$ , there is a successful run of the form

$$\rho' = X_0 \xrightarrow{\text{proj}_Q(\rho)(0)} X_1 \xrightarrow{\text{proj}_Q(\rho)(1)} X_2 \xrightarrow{\text{proj}_Q(\rho)(2)} X_3 \dots$$

(recall that states of  $\mathcal{A}_\varphi$  are sets of formulae)

## Synchronized product

- Satisfaction of  $\rho, 0 \models \varphi$  and  $proj_Q(\rho), 0 \models \varphi$  can be represented by **two** synchronized sequences:

$$\begin{array}{ccccccccccc}
 (q_0, \vec{x}_0) & \rightarrow & (q_1, \vec{x}_1) & \rightarrow & (q_2, \vec{x}_2) & \rightarrow & (q_3, \vec{x}_3) & \rightarrow & \dots & \models \varphi \\
 X_0 & \xrightarrow{q_0} & X_1 & \xrightarrow{q_1} & X_2 & \xrightarrow{q_2} & X_3 & \xrightarrow{q_3} & \dots & \models \varphi
 \end{array}$$

- To design a unique counter system synchronizing  $S$  and  $\mathcal{A}_\varphi$  with control states of the form  $(q_i, X_i)$ .
- To update the counter values according to the transitions from  $S$ .
- $S = (Q, n, \delta)$ ,  $\mathcal{A} = (\Sigma, Q', Q'_0, \delta', F)$  with  $\Sigma = Q$ .  
Synchronized product  $S \otimes \mathcal{A} = (Q'', n, \delta'')$ :
  - $Q'' = Q \times Q'$ ,
  - $(q_0, q'_0) \xrightarrow{\varphi} (q_1, q'_1) \stackrel{\text{def}}{\Leftrightarrow} q_0 \xrightarrow{\varphi} q_1 \in \delta \text{ and } q'_0 \xrightarrow{q_0} q'_1 \in \delta'$ .

# Reduction to repeated reachability

- CS  $\mathcal{S}$ ,  $(q, \vec{x})$  and formula  $\varphi \in \text{LTL}(Q)$ .
- BA  $\mathcal{A}_\varphi = (\Sigma, Q', Q'_0, \delta', F)$  s.t.  $\text{Models}(\varphi) = L(\mathcal{A}_\varphi)$ .
- Equivalence between (I) and (II):
  - (I)  $\exists$  infinite run  $\rho$  from  $(q, \vec{x})$  s.t.  $\rho, 0 \models \varphi$ .
  - (II) For some  $q_i \in Q'_0$  and  $(q'', q_f) \in Q \times F$ , there is an infinite run in  $\mathcal{S} \otimes \mathcal{A}_\varphi$  from  $((q, q_i), \vec{x})$  such that  $(q'', q_f)$  is repeated infinitely often.
- Model-checking is reduced to repeated reachability.

# Decidability

- Let  $C$  be a class of counter systems such that
  - 1 the control state repeated reachability problem is decidable,
  - 2  $C$  is closed under synchronized products with BA.

Then, existential model-checking problem restricted LTL( $\mathcal{Q}$ ) and to counter systems in  $C$  is decidable.

# Proof

- There is an infinite run  $\rho$  with initial configuration  $(q, \vec{x})$  such that  $\rho, 0 \models \varphi$  iff for some  $q_i \in Q'_0$  and  $(q'', q_f) \in Q \times F$ , there is an infinite run in  $\mathcal{S} \otimes \mathcal{A}_\varphi$  with initial configuration  $((q, q_i), \vec{x})$  such that  $(q'', q_f)$  is repeated infinitely often.
- Since both  $Q'_0$  and  $Q \times F$  are finite sets, the existence of a finite run  $\rho$  such that  $\rho, 0 \models \varphi$  can be verified by checking at most  $\text{card}(Q'_0) \times \text{card}(Q \times F)$  instances of the control state repeated reachability problem on the system  $\mathcal{S} \otimes \mathcal{A}_\varphi$ .
- By condition (2), such a system belongs also to  $\mathcal{C}$  and the target problem is decidable by condition (1).

**What about VASS?**

# EXPSpace upper bound

- Control state repeated reachability problem restricted to VASS can be solved in exponential space.

[Habermehl, ICATPN 97]

- Adaptation of Rackoff's proof for solving boundedness and covering in exponential space.
- Equivalence between the propositions below.
  - There is an infinite run with initial configuration  $(q, \vec{x})$  such that the control state  $q_f$  is repeated infinitely often.
  - there is a finite run  $(q_0, \vec{x}_0), \dots, (q_k, \vec{x}_k)$  such that
    - $(q_0, \vec{x}_0) = (q, \vec{x})$ ,
    - there is  $k' < k$  such that  $\vec{x}_{k'} \preceq \vec{x}_k$ ,
    - $q_k = q_{k'} = q_f$ .

# LTL model-checking

- Use of Dickson's Lemma: for any infinite sequence  $\vec{y}_0, \vec{y}_1, \dots$  of tuples in  $\mathbb{N}^n$ , there are  $i < j$  such that  $\vec{y}_i \preceq \vec{y}_j$ .
- The key argument to get the EXPSPACE upper bound is to show that  $k$  can be at most double-exponential in the size of the instance  $\mathcal{S}, (q, \vec{x}), q'$ .
- Model-checking problem restricted to LTL(Q) and to VASS is EXPSPACE-complete [Habermehl, ICATPN 97].

## Another logic expressing fairness

- TLF formulae ( $q \in \mathcal{Q}$  and  $c \in \mathbb{N}$ ):

$$q \mid x_i \geq c \mid \neg(x_i \geq c) \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \text{GF}\varphi$$

- TLF formulae are not closed under negations and the temporal properties are intersection or union of fairness conditions.
- Existential model-checking problem for TLF restricted to VASS is decidable [Jančar, TCS 90].
- Addition of  $F$  may lead to undecidability.  
[Howell & Rosier, TCS 89]
- Decidability/undecidability results for linear-time temporal logic on Petri nets can be found in [Esparza, CAAP'94]; e.g.,  $\text{LTL}(\mathcal{Q}) + x_i = 0$  is undecidable.

## What about reversal-bounded CA?

- Control state repeated reachability problem restricted to reversal-bounded counter automata is decidable.

[Dang & Ibarra & San Pietro, FSTTCS'01]

(see slides Day 4)

- A stronger result is shown since Presburger-definable atomic properties can be included while preserving decidability.
- **Corollary:** Existential model-checking problem restricted to  $LTL(Q)$  and to reversal-bounded CA is decidable.

**What about gainy counter automata?**

## Gainy counter automata are back!

- Gainy counter automaton: standard counter automaton  $(Q, n, \delta)$  such that for  $q \in Q$  and  $i \in [1, n]$ ,  $q \xrightarrow{\text{inc}(i)} q \in \delta$ .
- Alternative definition: to modify the one-step relation  $(q, \vec{x}) \xrightarrow{t}_g (q', \vec{x}')$   $\stackrel{\text{def}}{\Leftrightarrow}$  there are  $\vec{y}$  and  $\vec{y}'$  in  $\mathbb{N}^n$  such that  $\vec{x} \preceq \vec{y}$  and  $(q, \vec{y}) \xrightarrow{t} (q', \vec{y}')$  – perfect step – and  $\vec{y}' \preceq \vec{x}'$ .
- The control state reachability problem for gainy counter automata is decidable but with nonprimitive recursive complexity [Schnoebelen, IPL 02].
- The control state repeated reachability problem restricted to gainy counter automata is undecidable.
- Hence, model-checking problem restricted to  $\text{LTL}(\mathcal{Q})$  and to gainy counter automata is undecidable.

## Undecidability proof – Step I

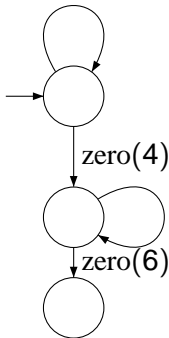
- Minsky machine  $\mathcal{S} = (Q, 2, \delta)$  with halting control state  $q_h$ .
- We have seen that the halting problem is undecidable.
- First, we build a CA  $\mathcal{S}' = (Q', 3, \delta')$  that behaves exactly as  $\mathcal{S}$  as far as the counters 1 and 2 are concerned.
- Counter 3 is incremented after each instruction of  $\mathcal{S}$ .
- Control state  $q_h$  cannot be reached in  $\mathcal{S}$  iff for the unique run of  $\mathcal{S}'$ , the counter 3 has no bounded value.

## Step II

- Gainy counter automaton  $S''$  with 6 counters:
  - The counters 1, 2 and 3 roughly behave as the 3 respective counters in  $S'$ .
  - Counter 4 is the global budget that is progressively incremented.
  - Counter 5 is the current budget. It records how many increments on one of the counters 1, 2 or 3 can be still performed.  
E.g., increment of counter 3 is followed by decrement of counter 5.
  - Counter 6 is auxiliary.
- We shall implement two subroutines:  $\text{copy}(4, 5)$  and  $\text{transfer}(1 + 2 + 3, 5)$

copy(4, 5) and transfer(1 + 2 + 3, 5)  
 (incrementating errors can occur)

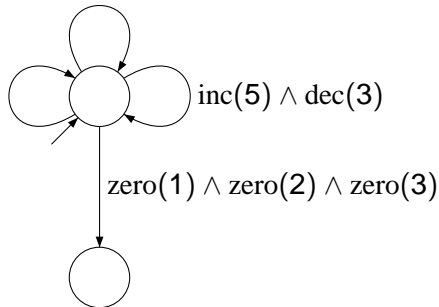
$\text{dec}(4) \wedge \text{inc}(5) \wedge \text{inc}(6)$



$\text{inc}(5) \wedge \text{dec}(2)$

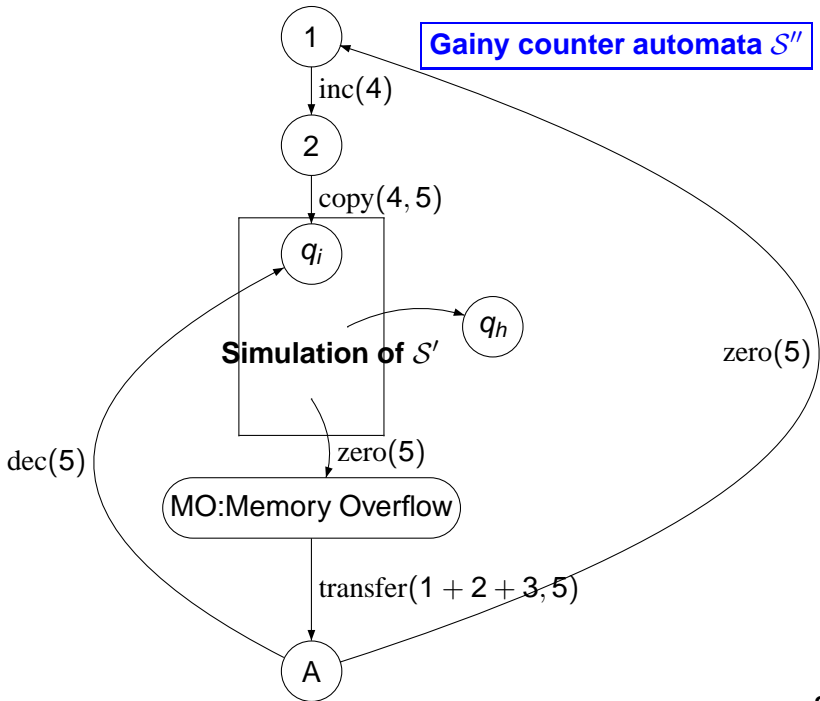
$\text{dec}(6) \wedge \text{inc}(4)$

$\text{inc}(5) \wedge \text{dec}(1)$



$\text{inc}(5) \wedge \text{dec}(3)$

$\text{zero}(1) \wedge \text{zero}(2) \wedge \text{zero}(3)$



## Simulation of $\mathcal{S}'$

- A transition  $q \xrightarrow{\text{dec}(i)} q'$  is simulated by  $q \xrightarrow{\text{dec}(i)} \circ \xrightarrow{\text{inc}(5)} q'$ . The location  $\circ$  is an arbitrary new location only used to simulate this transition.
- A transition  $q \xrightarrow{\text{zero}(i)} q'$  is simulated by itself.
- A transition  $q \xrightarrow{\text{inc}(i)} q'$  is simulated by  $q \xrightarrow{\text{inc}(i)} \circ \xrightarrow{\text{dec}(5)} q'$  and  $\circ \xrightarrow{\text{zero}(5)} \text{MO}$ .

## Non-reachability and repeated reachability

- One shall show that  $\mathcal{S}$  cannot reach  $q_h$  iff  $\mathcal{S}''$  visits infinitely often the control state (1).
- $\mathcal{S}$  cannot reach  $q_h$  iff  $\mathcal{S}'$  cannot reach  $q_h$ .
- If  $\mathcal{S}'$  cannot reach  $q_h$ , then an error-free run of  $\mathcal{S}''$  visits infinitely often (1).

## Converse direction

- Converse direction uses these facts:
  - In (A), the only way to decrement counter 5 is to simulate exactly  $S'$ .
  - In order to reach (1), in the part between  $q_i$  and (A), counter 5 is decremented regularly.
  - If  $S''$  visits infinitely often (1) and  $S'$  can reach some configuration  $(q_h, \vec{x})$ , then at some point an error-free simulation of  $S'$  shall be done with value for counter 5 greater than  $\vec{x}(1) + \vec{x}(2) + \vec{x}(3)$ , a contradiction.
- **Theorem:** control state repeated reachability problem restricted to gainy counter automata is undecidable.

# **Admissible Counter Systems**

# Overview

- Introduction to the class of admissible counter systems.
- Reachability relation is effectively semilinear.
- Existential model-checking problem for  $LTL^{CS}(\text{PrA})$  restricted to such counter systems is decidable.

# Affine functions

- Binary relation of dimension  $n$ : relation  $R \subseteq \mathbb{N}^{2n}$ .
- $R$  is Presburger definable  $\stackrel{\text{def}}{\Leftrightarrow}$  there is a Presburger formula  $\varphi(x_1, \dots, x_n, x'_1, \dots, x'_n)$  such that  $R = \text{REL}(\varphi)$ .

$$(\text{REL}(\varphi(x_1, \dots, x_k))) \stackrel{\text{def}}{=} \{(\mathbf{v}(x_1), \dots, \mathbf{v}(x_k)) \in \mathbb{N}^k : \mathbf{v} \models \varphi\}.$$

- Partial function  $f : \mathbb{N}^n \rightarrow \mathbb{N}^n$  is affine  $\stackrel{\text{def}}{\Leftrightarrow}$  there exist a matrix  $A \in \mathbb{Z}^{n \times n}$  and  $\vec{b} \in \mathbb{Z}^n$  such that for every  $\vec{a} \in \text{dom}(f)$ ,

$$f(\vec{a}) = A\vec{a} + \vec{b}$$

- $f$  is Presburger definable  $\stackrel{\text{def}}{\Leftrightarrow}$  the graph of  $f$  is a Presburger definable relation.

# Affine counter systems

- Affine counter system  $\mathcal{S} = (Q, n, \delta)$ : for every transition  $q \xrightarrow{\varphi} q' \in \delta$ ,  $\text{REL}(\varphi)$  is affine.
- $\varphi$  can be encoded by a triple  $(A, \vec{b}, \psi)$  such that
  - 1  $A \in \mathbb{Z}^{n \times n}$ ,
  - 2  $\vec{b} \in \mathbb{Z}^n$ ,
  - 3  $\psi$  has free variables  $x_1, \dots, x_n$ ,
  - 4  $\text{REL}(\varphi) = \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \vec{x}' = A\vec{x} + \vec{b} \text{ and } \vec{x} \in \text{REL}(\psi)\}$ .
- Guard  $\psi$  and deterministic update function  $(A, \vec{b})$ .
- Succinct counter automata are affine counter systems in which the matrices are equal to identity.

## Composing two affine updates

- Let  $(A_1, \vec{b}_1, \psi_1)$  and  $(A_2, \vec{b}_2, \psi_2)$  be two affine updates. There is  $(A, \vec{b}, \psi)$  such that

$$\begin{aligned} \text{REL}((A, \vec{b}, \psi)) = \\ \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \exists \vec{y} \in \mathbb{N}^n (\vec{x}, \vec{y}) \in \text{REL}((A_1, \vec{b}_1, \psi_1)) \\ \text{and } (\vec{y}, \vec{x}') \in \text{REL}((A_2, \vec{b}_2, \psi_2))\} \end{aligned}$$

- $A = A_2 A_1$ .
- $\vec{b} = A_2 \vec{b}_1 + \vec{b}_2$ .
- $\psi = \exists \vec{y} \psi_1(\vec{x}) \wedge \vec{y} = A_1 \vec{x} + \vec{b}_1 \wedge \psi_2(\vec{y})$ .

# Loop effect

$(A, \vec{b}, \psi)$



- How to represent symbolically  
 $X = \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : (q, \vec{x}) \xrightarrow{*} (q, \vec{x}')\}$ ?
- Is  $X$  definable in Presburger arithmetic?
- Reflexive and transitive closure  $R^* \subseteq \mathbb{N}^{2n}$  of  $R \subseteq \mathbb{N}^{2n}$ :  
 $(\vec{y}, \vec{y}') \in R^*$  iff there are  $\vec{x}_1, \dots, \vec{x}_k \in \mathbb{N}^n$  such that
  - $\vec{x}_1 = \vec{y}$ ,
  - $\vec{x}_k = \vec{y}'$ ,
  - for  $i \in [1, k - 1]$ , we have  $(\vec{x}_i, \vec{x}_{i+1}) \in R$ .

## Loop effect (II)

- If  $R$  is Presburger definable, this does not imply that  $R^*$  is Presburger definable too.
- $R = \{(\alpha, 2\alpha) \in \mathbb{N}^2 : \alpha \in \mathbb{N}\}$ .
  - $R^* = \{(\alpha, 2^\beta \alpha) \in \mathbb{N}^2 : \alpha, \beta \in \mathbb{N}\}$ .
  - If  $R^*$  is Presburger definable, then so is  $\{2^\beta \in \mathbb{N} : \beta \in \mathbb{N}\}$ .
  - Semilinear subset of  $\mathbb{N}$  are ultimately periodic.
  - $\rightarrow R^*$  is not Presburger definable.
- If  $S = \{(\alpha, \alpha + 1) \in \mathbb{N}^2 : \alpha \in \mathbb{N}\}$  then  $S^* = \{(\alpha, \beta) \in \mathbb{N}^2 : \alpha < \beta, \alpha, \beta \in \mathbb{N}\}$  is Presburger definable.

## Presburger counting iteration

- The counting iteration of  $R \subseteq \mathbb{N}^{2n}$  is  $R_{\text{CI}} \subseteq \mathbb{N}^n \times \mathbb{N} \times \mathbb{N}^n$  such that  $(\vec{a}, i, \vec{b}) \in R_{\text{CI}}$  iff  $(\vec{a}, \vec{b}) \in R^i$ .
- $R$  has a Presburger counting iteration if its counting iteration is Presburger definable.
- $\{(\alpha, \alpha + 1) \in \mathbb{N}^2 : \alpha \in \mathbb{N}\}$  has a Presburger counter iteration.
- For  $A \in \mathbb{Z}^{n \times n}$ ,  $A^*$  denotes the monoid generated from  $A$  with  $A^* = \{A^i : i \in \mathbb{N}\}$ .
- The identity element is  $A^0 = I$ .
- Given  $A \in \mathbb{Z}^{n \times n}$ , checking whether the monoid generated by  $A$  is finite, is decidable [Mandel & Simon, TCS 77].

# Main result

- Let  $R = \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \vec{x}' = A\vec{x} + \vec{b} \text{ and } \vec{x} \in \text{REL}(\psi)\}$ .
- **Theorem:** If  $A^*$  is finite, then  $R$  has a Presburger counting iteration.

[Boigelot, PhD 98; Finkel & Leroux, FSTTCS'02]

- In CA,  $A$  is the identity and therefore  $A^*$  is finite.
- General thema in the literature to determine when Presburger definable relations admit Presburger definable reflexive and transitive closure.

## Proof – Preliminaries

- Let  $R \subseteq \mathbb{N}^{2n}$  be defined by  $(A, \vec{b}, \psi)$ .
- $g$ : affine update function obtained by ignoring the guard  $\psi$ .

$$g(\vec{a}) = A\vec{a} + \vec{b}$$

- Since  $A^*$  is finite, there are  $\alpha, \beta \in \mathbb{N}$  such that  $A^{\alpha+\beta} = A^\alpha$ .
- $\alpha$  and  $\beta$  can be effectively computed from  $A$ .

[Mandel & Simon, TCS 77]

- Simple equalities ( $k \geq 1$ ):
  - $g^k(\vec{a}) = A^k\vec{a} + A^{k-1}\vec{b} + \dots + \vec{b}$ .
  - $g^k(\vec{0}) = A^{k-1}\vec{b} + \dots + \vec{b}$ .

## Proof – Vectors of terms

- Terms in Presburger Arithmetic:

$$t ::= 0 \mid 1 \mid x \mid t + t$$

- Given an  $n$ -tuple  $\vec{t}$  of terms,  $g^k(\vec{t})$  denotes the  $n$ -tuple

$$A^k \vec{t} + A^{k-1} \vec{b} + \dots + \vec{b}$$

- $\psi(\vec{t})$  is a shortcut for the Presburger formula

$$\exists \mathbf{x}_1, \dots, \mathbf{x}_n \psi(\mathbf{x}_1, \dots, \mathbf{x}_n) \wedge \left( \bigwedge_{i \in [1, n]} \mathbf{x}_i = \vec{t}(i) \right)$$

$$\vec{t} = \begin{pmatrix} 2 & -2 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ -2 \end{pmatrix} = \begin{pmatrix} 2x - 2y + 1 \\ -3x + 7y - 2 \end{pmatrix}$$

$$\psi(\vec{t}) \stackrel{\text{def}}{=} \exists \mathbf{x}_1, \dots, \mathbf{x}_n \psi(\mathbf{x}_1, \dots, \mathbf{x}_n) \wedge x_1 + 2y = 2x + 1 \wedge x_1 + 3x + 2 = 7y$$

# Proof – Quantifying over number of compositions

- $(\vec{x}, \vec{x}') \in R^*$  iff there is  $i \geq 0$  such that

- 1  $\vec{x}' = g^i(\vec{x})$ ,
- 2 for  $0 \leq j < i$ ,  $g^j(\vec{x}) \models \psi$ .

- Presburger formula defining  $R^*$  may look like

$$\exists i \vec{x}' = g^i(\vec{x}) \wedge \bigwedge_{j < i} \psi(g^j(\vec{x})).$$

- But,

- 1  $g^i(\vec{x})$  is a shortcut for  $A^i\vec{x} + A^{i-1}\vec{b} + \dots + \vec{b}$ ,
- 2 generalized conjunction has exactly  $i$  conjuncts.

- $\vec{x}' = g^i(\vec{x}) \wedge \bigwedge_{j < i} \psi(g^j(\vec{x}))$  defines a family of formulae rather than a single formula.

## Proof – Transforming an exponent into a factor

- Use  $A^{\alpha+\beta} = A^\alpha$  to replace  $i$  applications of  $g$  by expressions in which  $i$  appears as a variable.
- For  $q \geq 1$ , we shall show  $g^{\alpha+q\beta}(\vec{a}) = g^\alpha(\vec{a}) + qA^\alpha g^\beta(\vec{0})$ .
- $q$  becomes a factor and  $A^\alpha g^\beta(\vec{0})$  is constant tuple.
- For  $i - \alpha = r + q\beta$  with  $r < \beta$  and  $i \geq \alpha$ ,

$$g^i(\vec{a}) = g^r(g^\alpha(\vec{a}) + qA^\alpha g^\beta(\vec{0})).$$

$$\text{(Proof – } g^{\alpha+q\beta}(\vec{a}) = g^\alpha(\vec{a}) + qA^\alpha g^\beta(\vec{0})\text{)}$$

- Preliminary identities:

$$\begin{aligned} g^{\alpha+\beta}(\vec{a}) &= A^{\alpha+\beta}\vec{a} + A^{\alpha+\beta-1}\vec{b} + \dots + \vec{b}. \\ &= A^{\alpha+\beta}\vec{a} + A^\alpha(A^{\beta-1}\vec{b} + \dots + \vec{b}) + (A^{\alpha-1}\vec{b} + \dots + \vec{b}) \\ &= A^\alpha\vec{a} + A^\alpha g^\beta(\vec{0}) + (A^{\alpha-1}\vec{b} + \dots + \vec{b}) \\ &= g^\alpha(\vec{a}) + A^\alpha g^\beta(\vec{0}). \end{aligned}$$

- Case  $q = 1$  is above.
- $g^{\alpha+(q+1)\beta}(\vec{a}) = g^\alpha(g^\beta(\vec{a})) + qA^\alpha g^\beta(\vec{0})$ .
- $g^{\alpha+(q+1)\beta}(\vec{a}) = g^\alpha(\vec{a}) + A^\alpha g^\beta(\vec{0}) + qA^\alpha g^\beta(\vec{0})$ .
- $g^{\alpha+(q+1)\beta}(\vec{a}) = g^\alpha(\vec{a}) + (q+1)A^\alpha g^\beta(\vec{0})$ .

## Proof – Towards the final formula

- For fixed  $i \geq 0$ , let  $R[i]$  be such that

$$\text{REL}(R[i]) = \{(\vec{y}, \vec{y}') \in \mathbb{N}^{2n} : \vec{y}' R^i \vec{y}\}$$

- $R[0]$  is equal to  $\bigwedge_{j \in [1, n]} x_j = x'_j$ .
- $R[i + 1]$  is equal to  $\exists \vec{y} \psi(\vec{y}) \wedge R[i](\vec{x}, \vec{y}) \wedge \vec{x}' = A\vec{y} + \vec{b}$ .
- To show that  $R$  has a Presburger counting iteration, we define  $\chi(\vec{x}, z, \vec{x}')$  such that  $R_{\mathbf{CI}} = \text{REL}(\chi(\vec{x}, z, \vec{x}'))$ .
- $\chi(\vec{x}, z, \vec{x}')$  is equal to:

$$((z = 0 \wedge R[0]) \vee \cdots \vee (z = \alpha - 1 \wedge R[\alpha - 1])) \vee$$

$$(z \geq \alpha \wedge \exists \mathbf{q} (\chi_{\mathbf{q}, 0} \vee \cdots \vee \chi_{\mathbf{q}, \beta - 1}))$$

## Proof – Defining the last chunks

- $\chi_{q,r}$  is equal to  $(z - \alpha = r + \beta \times q) \wedge$   
 $(\exists \vec{y}' \vec{y}' = A^\alpha \vec{x} + q A^\alpha (A^{\beta-1} \vec{b} + \dots + \vec{b})) \wedge \vec{x}' = g^r(\vec{y}')) \wedge \chi^{\text{guard}}(z, \vec{x})$
- This encodes  $g^i(\vec{a}) = g^r(g^\alpha(\vec{a}) + q A^\alpha g^\beta(\vec{0}))$  and the point below.
- $\chi^{\text{guard}}(z, \vec{x})$  checks that the guard is satisfied for all the intermediate configurations.

$$\chi^{\text{guard}}(z, \vec{x}) \stackrel{\text{def}}{=} \left( \bigwedge_{i \in [1, \alpha]} \exists \vec{y} \text{R}[i](\vec{x}, \vec{y}) \right) \wedge \forall z' \alpha \leq z' < z \Rightarrow$$

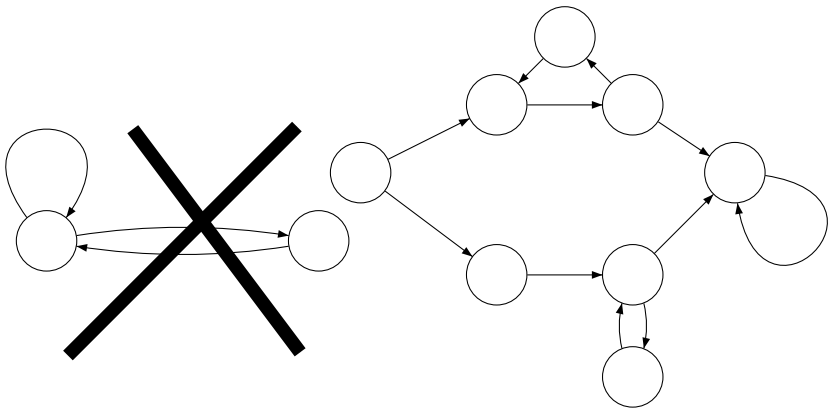
$$\bigvee_{r' \in [1, \beta-1]} \exists q' (z' - \alpha = r' + q' \beta \wedge (\exists \vec{y}' \vec{y}' = A^\alpha \vec{x} + q' A^\alpha (A^{\beta-1} \vec{b} + \dots + \vec{b})) \wedge \psi(g^{r'}(\vec{y}'))))$$

# Admissible counter systems

- A loop in an affine counter system has the finite monoid property  $\stackrel{\text{def}}{\iff} A^*$  is finite for its corresponding affine update  $(A, \vec{b}, \psi)$ .
- Admissible counter system  $\mathcal{S}$ :
  - 1  $\mathcal{S}$  is an affine counter system,
  - 2 there is at most one transition between two control states,
  - 3 its control graph is flat,
  - 4 each loop has the finite monoid property.
- Consequently, the effect of each loop can be defined in Presburger Arithmetic.

## Flatness

A CS is flat if every control state belongs to at most one simple cycle. Moreover, there is at most one transition between two control states.



## Reachability is semilinear !

- Let  $\mathcal{S}$  be an admissible counter system and  $q, q' \in Q$ . One can effectively compute  $\varphi$  such that for every  $\mathbf{v}$ , we have  $\mathbf{v} \models \varphi$  iff  $(q, (\mathbf{v}(x_1), \dots, \mathbf{v}(x_n))) \xrightarrow{*} (q', (\mathbf{v}(x'_1), \dots, \mathbf{v}(x'_n)))$ .

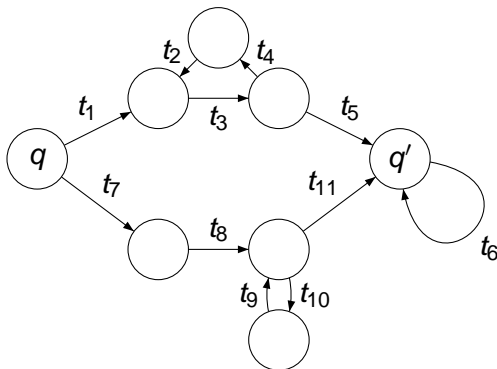
[Finkel & Leroux, FSTTCS'02; Leroux, PhD 03]

- First, build FSA  $\mathcal{A}$  that overapproximates the language of transitions between  $q$  and  $q'$  (ignore counter values).

# Proof

- The language of transitions between  $q$  and  $q'$  can be approximated by the union below ( $\Sigma = \delta$ ):

$$t_1 t_3 (t_4 t_2 t_3)^* t_5 t_6^* \cup t_7 t_8 (t_{10} t_9)^* t_{11} t_6^*$$



- By flatness,  $L(\mathcal{A})$  is a finite union of languages of the form  $u_1(v_1)^* u_2(v_2)^* \cdots (v_k)^* u_{k+1}$  with  $u_i \in \Sigma^*$  and  $v_i \in \Sigma^+$ .

## Proof – Glueing pieces

- We know that there is a Presburger formula that encodes the effect of applying a finite number of times the loop  $v_i$ .
- We also know that there is a Presburger formula that encodes the effect of applying once the segment  $u_i$ .
- One can effectively compute the effect of applying a sequence of transitions in the language  $L$ .  
(use existential quantification for intermediate positions)
- Since  $L(\mathcal{A})$  is a finite union of bounded languages and Presburger arithmetic has obviously disjunction, there is  $\varphi(\vec{x}, \vec{x}')$  such that for  $\mathbf{v}$ , we have

$$\mathbf{v} \models \varphi \text{ iff } (q, (\mathbf{v}(x_1), \dots, \mathbf{v}(x_n))) \xrightarrow{*} (q', (\mathbf{v}(x'_1), \dots, \mathbf{v}(x'_n)))$$

## About flatness

- Flat CS are not widely spread in real-life applications.
- A relaxed version of flatness: reachability can be captured by a flat unfolding of the system.
- $(\mathcal{S}, (q, \vec{x}))$  is flattable whenever there is a partial unfolding of  $(\mathcal{S}, (q, \vec{x}))$  that is flat and has the same reachability set as  $(\mathcal{S}, (q, \vec{x}))$ .

- $\Sigma = \delta$ ; let L be a finite union of languages of the form

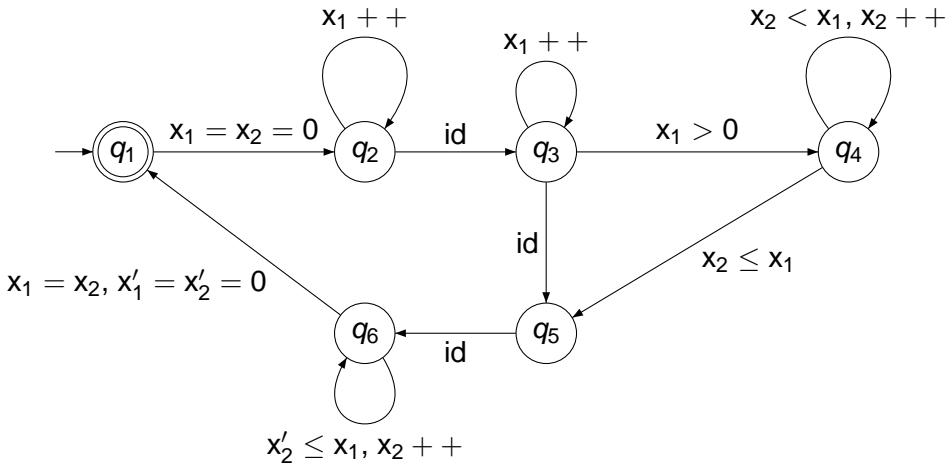
$$u_1(v_1)^* u_2(v_2)^* \cdots (v_k)^* u_{k+1},$$

such that two consecutive transitions share the intermediate control state.

- $(\mathcal{S}, (q, \vec{x}))$  is initially flattable iff there is some L of the above form such that

$$\{(q', \vec{x}') : (q, \vec{x}) \xrightarrow{*} (q', \vec{x}')\} = \{(q', \vec{x}') : (q, \vec{x}) \xrightarrow{u} (q', \vec{x}'), u \in L\}$$

Is  $(\mathcal{S}, (q_1, \vec{0}))$  initially flattable?



## On being globally flappable

- $\mathcal{S}$  is globally flappable  $\stackrel{\text{def}}{\iff}$  there is a finite union of bounded languages  $L$  such that

$$\xrightarrow{*} = \{((q, \vec{x}), (q', \vec{x}')) : (q, \vec{x}) \xrightarrow{u} (q', \vec{x}'), u \in L\}$$

- Flappable counter systems are everywhere.  
[Leroux & Sutre, ATVA'05]
  - Globally reversal-bounded CA are globally flappable.
  - Reversal-bounded initialized CA are initially flappable.
  - Initialized gainy CA are initially flappable.
- Semilinearity for reversal-bounded CA is regained:
  - $L$  can be effectively computed.
  - Initialized CA +  $L$  leads to an admissible counter system.
  - Reachability relation for admissible CS is semilinear.

# Decidable model-checking problem

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

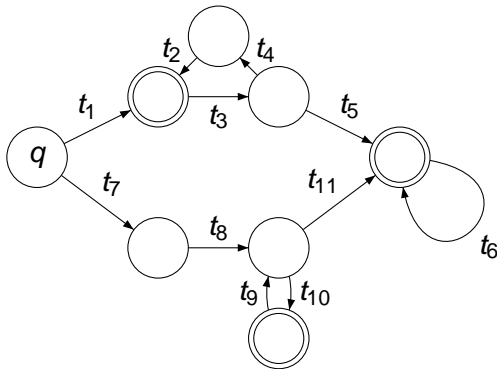
$$\varphi ::= \psi \mid \mathbf{q} \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathbf{x}\varphi \mid \varphi \mathbf{U}\varphi \mid \exists \mathbf{y} \varphi$$

- **Theorem:** Existential model-checking problem for  $LTL^{CS}(\text{PrA})$  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.

## Proof – Showing a stronger property

- Instance:  $\mathcal{S} = (Q, n, \delta), (q, \vec{x}), \varphi$ .
- 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  $\text{card}(Q)$ .
- 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:

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

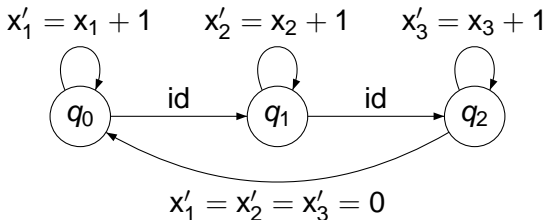
# From FO-definable temporal operators to FO on $(\mathbb{N}, +)$

- $t_L$  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  $\text{VAR}^p$ .

## Open problems

- Computational complexity of the model-checking problem for  $LTL^{CS}(\text{PrA})$  restricted to ACS is still open.
- Decidability extends to a  $CTL^*$  extension of  $LTL^{CS}(\text{PrA})$ .  
What about the linear  $\mu$ -calculus extension?
- Which conditions in the presented definition of admissible counter systems can be relaxed so that the model-checking problem for  $LTL^{CS}(\text{PrA})$  remains decidable?
- ... but a slight relaxation can lead to undecidability.

# Undecidable model-checking problem



- Existential model-checking problem for  $LTL^{CS}(\text{PrA})$  restricted to the affine counter system  $\mathcal{S}_U$  is undecidable.
- Reduction from the recurrence problem for ND Minsky machines.

# Concluding remarks for Day 5

- Today's lecture:
  - Repeated reachability problem for several classes.
  - Plain LTL for several classes of counter systems.
  - $\text{LTL}^{\text{CS}}(\text{PrA})$  for admissible counter systems.
- We have illustrated two proof techniques:
  - 1 Combining repeated reachability with standard automata-based approach for temporal logics.
  - 2 Translation into the decidable Presburger Arithmetic.

## Further topics

- Theory of well-structured transition systems.  
[Finkel & Schnoebelen, TCS 01]
- Decidability of reachability for VASS.  
[Reutenauer, Book 90]
- Recent developments on classes of counter systems with semilinear reachability relations.
- Computational complexity of reachability and model-checking problems.

## Further topics (II)

- Decision procedures for Presburger Arithmetic.
- Applications:
  - Verification of broadcast protocols.  
[Esparza & Finkel & Mayr, LICS'99]
  - Program with pointers [Sangnier, PhD 08].
  - Thread-state reachability problem for replicated finite-state programs [Kaiser & Kroening & Wahl, CAV'10].
  - etc.

## A few current trends

- Transition closures of integer relations.  
See e.g. [Bozga & Josif & Konečný, CAV'10]
- SMT solvers for model-checking infinite-state systems.  
See e.g. [Ghilardi et al., CAV'07]
- Adding branching to VASS, leading to BVASS.  
See e.g. [Verma & Goubault-Larrecq, DMTCS 05]
- Relationships between counter automata and data logics.  
See e.g. [Bojańczyk & Lasota, LICS'10]