Decidability and complexity issues for subclasses of counter systems

Lecture 4
Counter automata with finite monoid property and flatness

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 lectures: VASS, reversal-bounded CA.

- Today’s lecture:
  - Other reachability problems for reversal-bounded CA.
  - Affine counter systems with flatness and finite monoid property. Reachability sets are effectively semilinear.

- Exercises.
Repeated reach. pb. for reversal-bounded CA
Reminder (see previous lecture)

**Theorem:** Let \((S, (q_0, \vec{x}))\) be \(r\)-reversal-bounded for some \(r \geq 0\). For each control state \(q_f\), the set

\[
R = \{ \vec{y} \in \mathbb{N}^n : \exists \text{ run } (q_0, \vec{x}) \xrightarrow{*} (q_f, \vec{y}) \}
\]

is effectively semilinear.

... but this result is not sufficient to answer questions about existence of infinite runs satisfying specific properties!
Decidability

- Control state repeated reachability problem restricted to reversal-bounded initialized counter automata is decidable. 
  [Dang & Ibarra & San Pietro, FSTTCS’01]

- $\exists$-Presburger infinitely often problem
  
  **Input:** Initialized CA $(S, (q, \bar{x}))$ of dimension $n$ that is $r$-reversal-bounded and a temporal formula of the form $\psi = GF \varphi(x_1, \ldots, x_n)$ where $\varphi$ is a Presburger formula on counters.
  
  **Question:** Is there an infinite run from $(q, \bar{x})$ satisfying $\psi$?

- $\exists$-Presburger infinitely often problem is decidable. 
  [Dang & San Pietro & Kemmerer, TCS 03]
Proof for the decidability of control state repeated reachability problem

- $r$-reversal-bounded initialized CA $(S, (q_0, \vec{x}_0))$ and $q_f \in Q$.
- Property ($\star$): there is an infinite run from $(q_0, \vec{x}_0)$ such that $q_f$ is repeated infinitely often.
- We reduce ($\star$) to a reachability question for a new reversal-bounded counter automaton $S'$.
- Property ($\star\star$): there exists a finite run $(q_0, \vec{x}_0) \xrightarrow{t_1} (q_1, \vec{x}_1) \cdots \xrightarrow{t_{l'}} (q_{l'}, \vec{x}_{l'}) \cdots \xrightarrow{t_l} (q_l, \vec{x}_l)$ such that
  1. $q_l = q_{l'} = q_f$,
  2. $\vec{x}_{l'} \preceq \vec{x}_l$,
  3. if $X \subseteq [1, n]$ is the set of counters tested to zero between $(q_l, \vec{x}_l)$ and $(q_{l'}, \vec{x}_{l'})$, then $\vec{x}_{l'}(X) = \vec{x}_l(X) = \vec{0}$. 
Equivalence

- (⋆) is equivalent to (⋆⋆).
- (⋆⋆) shall provide a characterization with a finite witness run that can be encoded as a reachability question.
- (⋆⋆) implies (⋆):
  - \( \rho = (q_0, \vec{x}_0) \xrightarrow{t_1} (q_1, \vec{x}_1) \cdots \xrightarrow{t_{l'}} (q_{l'}, \vec{x}_{l'}) \cdots \xrightarrow{t_l} (q_l, \vec{x}_l) \).
  - Infinite \( \rho' \) is defined with \( t_1 \cdots t_{l'} (t_{l'+1} \cdots t_l)^\omega \).
  - \( q_f \) is repeated infinitely often.
  - Zero-tests are also successful (why?).
(⋆) implies (⋆⋆)

- $\rho = (q_0, x_0) \xrightarrow{t_1} (q_1, x_1) \xrightarrow{t_2} (q_2, x_2) \cdots$ with $q_f$ repeated infinitely often.

- $X$: set of counters that are successfully tested to zero in $\rho$ infinitely often.

- By reversal-boundedness, there is $I \geq 0$ s.t. for $k \geq I$, we have $\vec{x}_k(X) = \vec{0}$.

- There exists $l \leq k_1 < k_2 < k_3 < \ldots$ s.t. for $1 \leq j < j'$, we have $q_{k_j} = q_f$ and between $(q_{k_j}, x_{k_j})$ and $(q_{k_{j'}}, x_{k_{j'}})$, exactly the counters in $X$ are tested to zero.

- By Dickson’s Lemma, there exists $J < J'$ such that $\vec{x}_{k_j} \preceq \vec{x}_{k_{j'}}$. 
Reduction to a reachability question

\[ S' = (Q', q_0, 3 \times n, \delta') \text{ s.t. } (\ast \ast) \text{ iff } (q_0, \vec{x}_0) \overset{*}{\rightarrow} (q_{\text{new}}, \vec{0}) \text{ in } S'. \]

\[ \begin{align*}
S' & = (Q', q_0, 3 \times n, \delta') \\
& \text{s.t. } (\ast \ast) \text{ iff } (q_0, \vec{x}_0) \overset{*}{\rightarrow} (q_{\text{new}}, \vec{0}) \text{ in } S'.
\end{align*} \]

\[ S_X = S \setminus \text{zero-tests for } \overline{X} \]

\[ \overline{X} \overset{\text{def}}{=} [1, n] \setminus X \]

\[ S_X = S \setminus \text{zero-tests for } \overline{X} \]

\[ \overline{X} \overset{\text{def}}{=} [1, n] \setminus X \]

\[ S_X = S \setminus \text{zero-tests for } \overline{X} \]

\[ \overline{X} \overset{\text{def}}{=} [1, n] \setminus X \]
Construction of $S'$

- Let $S' = (Q', q_0, 3 \times n, \delta')$ s.t. $(\ast \ast)$ iff $(q_0, \vec{x}_0) \xrightarrow{\ast} (q_{\text{new}}, \vec{0})$ in $S'$.

- Essentially, runs for $S'$ are also runs for $S$.

- One can effectively build $\varphi$ s.t.
  $$\text{REL}(\varphi) = \{ \vec{x} : (q_0, \vec{x}_0) \xrightarrow{\ast} (q_{\text{new}}, \vec{x}) \text{ in } S' \}$$

- $S'$ is made of $2^n + 1$ copies of $S$ plus some extra control states such as $q_{\text{new}}$.

- It includes an initial distinguished copy of $S$.

- For $X \subseteq [1, n]$, the control states of the $X$-copy ($S_X$) are among $Q \times \{X\} \times \mathcal{P}(X)$.

- Third component records the counters that have been tested to zero since the run has entered in the $X$-copy.
Entering into the $X$-copy

• For $X \subseteq [1, n]$, we consider a sequence of transitions from $q_f$ to $(q_f, X, \emptyset)$ whose effect is to perform a zero-test on counters in $X$ and to copy the value of each counter $i \in X$ into the counter $n + i$.

• copy $x_i \to x_{i+n}$:
  1. Decrement the counter $i$ until zero and for each decrement, the counters $n + i$ and $2n + i$ are incremented.
  2. When counter $i$ is equal to zero, decrement the counter $2n + i$ until zero while incrementing the counter $i$ at each step.
  3. The number of reversals is at most augmented by 2.
Transitions in the $X$-copy

- $(q, X, Y) \xrightarrow{\varphi} (q', X, Y')$ is a transition whenever there is a transition $q \xrightarrow{\varphi'} q'$ in $S$ for which
  - $\varphi$ performs the same instruction as $\varphi'$,
  - for $i \in \overline{X}$, $\varphi'$ is a not a zero-test on $i$,
  - if $\varphi = \text{zero}(j)$, then $Y' = Y \cup \{j\}$ otherwise $Y' = Y$.

- When all the counters in $X$ have been tested to zero at least once and $q_f$ is reached, we may jump to $q_{new}$.
Final step

- Consider a sequence of transitions from \((q_f, X, X)\) to \(q_{new}\) performing the following tasks:

  1. for \(i \in X\), perform a zero-test on counter \(i\),

  2. for \(i \in \overline{X}\), test whether the counter value for \(i\) is greater or equal to the counter value for \(n + i\),

  3. empty all the counters.

- check \(x_{i+n} \leq x_i\): decrement \(i\) and \(n + i\) simultaneously and nondeterministically test whether the counter \(n + i\) has value zero.

- \((S', (q_0, \vec{x}_0))\) is \((r + 3)\)-reversal-bounded.
Undecidable Model-Checking Problems
Universal problem for one-counter automaton

- One-counter automaton with alphabet: FSA + 1 counter.
- The universal problem for 1-reversal-bounded one-counter automata with alphabet is undecidable \([\text{Ibarra, MST 79}].\)
- One-counter automata with alphabet defines context-free languages.
A simple undecidable temporal fragment

- The $\exists$-Presburger-always problem:
  
  **Input:** Initialized CA $(S, (q, \vec{x}))$ that is $r$-reversal-bounded and a formula 
  
  $\psi = G\varphi(x_1, \ldots, x_n)$ where $\varphi$ is a Presburger formula on counters.

  **Question:** Is there an infinite run from $(q, \vec{x})$ satisfying $\psi$?

- The $\exists$-Presburger-always problem for reversal-bounded counter automata is undecidable. 
  
  [Dang & San Pietro & Kemmerer, TCS 03]

- By reduction from halting problem for Minsky machines: one counter is encoded by two increasing counters, counting the number of increments and decrements, respectively.
**Reduction from the halting problem**

- Proof analogous to the undecidability of the reachability problem for reversal-bounded CA augmented with guards $x_i = x_{i'}$ and $x_i \neq x_{i'}$. [Ibarra et al., TCS 02]

- Given a Minsky machine $S$ with halting state $q_h$, we build a 0-reversal-bounded counter automaton $S'$ such that
  - counter $i$ in $S'$ records the increments of counter $i$ in $S$,
  - counter $i + 2$ in $S'$ records the decrements of counter $i$ in $S$.
  - zero-test on counter $i$ in $S$ is simulated by formula $x_i = x_{i+2}$.

- W.l.o.g., we can assume that
  - $S = (Q, 2, \delta)$ is a deterministic CA,
  - Halting control states in $Q_h \subseteq Q$ (no outgoing transitions),
  - $Q_1, Q_2 \subseteq Q$ contains exactly the control states that are reached after zero-tests on counter 1 and counter 2, respectively.
Building $S'$ by erasing zero-tests

- 0-reversal-bounded CA $S' = (Q, 5, \delta')$:
  - $q^{\text{inc}(i)} \xrightarrow{\text{inc}(i)} q' \in \delta$ implies $q^{\text{inc}(i)} \xrightarrow{\text{inc}(i)} q' \in \delta'$.
  - $q^{\text{dec}(i)} \xrightarrow{\text{dec}(i)} q' \in \delta$ implies $q^{\text{inc}(i+2)} \xrightarrow{\text{inc}(i+2)} q' \in \delta'$.
  - $q^{\text{zero}(i)} \xrightarrow{\text{zero}(i)} q' \in \delta$ implies $q^{\text{inc}(5)} \xrightarrow{\text{inc}(5)} q' \in \delta'$.

- No halting control state is reached from $(q, \vec{0})$ in $S$ iff there is an infinite run from $(q, \vec{0})$ in $S'$ satisfying

$$
\begin{align*}
G\left( \bigwedge_{i \in \{1, 2\}} \bigwedge_{q \in Q_i} (q \Rightarrow x_i = x_{i+2}) \right) & \land G\left( \bigwedge_{i \in \{1, 2\}} x_i \geq x_{i+2} \right) \land G\left( \bigwedge_{q \in Q_h} \neg q \right)
\end{align*}
$$

- Control states can be eliminated by adding increasing counters whose differences encode control states.
Affine counter systems with finite monoid property
Overview

• Introduction to the class of admissible counter systems.

• Reachability relation is effectively semilinear.

• First part of next lecture: decidability of Presburger LTL model-checking over the class of admissible counter systems.
Counter systems (bis)

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

- Counter system \( S = (Q, n, \delta) \) of dimension \( n \geq 1 \):
  - \( Q \) is a nonempty finite set of control states.
  - \( \delta \): finite set of transitions of the form \( t = (q, \varphi, q') \) where \( q, q' \in Q \) and \( \varphi \) is a Presburger formula with free variables \( x_1, \ldots, x_n, x'_1, \ldots, x'_n \).

- Configuration \( (q, \vec{a}) \in Q \times \mathbb{N}^n \).

- \( (q, \vec{a}) \overset{t}{\rightarrow} (q', \vec{a}') \) \( \overset{\text{def}}{=} \) \( v[\vec{x} \leftarrow \vec{a}, \vec{x}' \leftarrow \vec{a}'] \models \varphi \).

- Runs as nonempty (possibly infinite) sequences
  \[ \rho = (q_0, \vec{a}_0) \rightarrow (q_1, \vec{a}_1) \cdots (q_k, \vec{a}_k) \cdots \]
Subclasses of counter systems (bis)

- Standard counter automaton \((Q, n, \delta)\): transitions are of the form either \(q \xrightarrow{\text{inc}(i)} q'\) or \(q \xrightarrow{\text{dec}(i)} q'\) or \(q \xrightarrow{\text{zero}(i)} q'\).

- Succinct counter automaton \((Q, n, \delta)\): transitions of the form either \(q \xrightarrow{\text{add}(\vec{b})} q'\) with \(\vec{b} \in \mathbb{Z}^n\) or \(q \xrightarrow{\text{zero}(\vec{b}')} q'\) with \(\vec{b}' \in \{0, 1\}^n\) (simultaneous zero-tests).

- Affine counter systems are counter systems, generalizing the class of succinct counter automata.

- Hence, most reachability/verification problems are undecidable but we shall impose some further restrictions.
**Affine functions**

- Binary relation of dimension $n$: relation $R \subseteq \mathbb{N}^{2n}$.

- $R$ is Presburger definable $\iff$ there is a Presburger formula $\varphi(x_1, \ldots, x_n, x'_1, \ldots, x'_n)$ such that $R = \text{REL}(\varphi)$.

\[
(\text{REL}(\varphi(x_1, \ldots, x_k))) \overset{\text{def}}{=} \{(v(x_1), \ldots, v(x_k)) \in \mathbb{N}^k : v \models \varphi\}.
\]

- Partial function $f : \mathbb{N}^n \to \mathbb{N}^n$ is affine $\iff$ 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 $\iff$ 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.

- Herein, $\varphi$ is 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 $x_1, \ldots, x_n$,
  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.
One step relation is semilinear (easy)

- Assuming $t = q \xrightarrow{(A, \vec{b}, \psi)} q'$, there is a Presburger formula $\chi(\vec{x}, \vec{x}')$ such that for every $v$, we have $v \models \chi$ iff

\[
(q, (v(x_1), \ldots, v(x_n))) \xrightarrow{t} (q', (v(x'_1), \ldots, v(x'_n))).
\]

\[
\psi(\vec{x}) \land \bigwedge_{i \in [1,n]} (x'_i = \sum_j A(i,j)x_j + \vec{b}(i))
\]
Composing two affine updates

\[
\begin{pmatrix}
  x'_1 \\
  x'_2
\end{pmatrix} = \begin{pmatrix}
  1 & 0 \\
  0 & 1
\end{pmatrix} \begin{pmatrix}
  x_1 \\
  x_2
\end{pmatrix} + \begin{pmatrix}
  3 \\
  -3
\end{pmatrix}
\]

\[
\begin{pmatrix}
  x'_1 \\
  x'_2
\end{pmatrix} = \begin{pmatrix}
  2 & 0 \\
  0 & 2
\end{pmatrix} \begin{pmatrix}
  x_1 \\
  x_2
\end{pmatrix} + \begin{pmatrix}
  -1 \\
  2
\end{pmatrix}
\]
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

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

- Partial \(f_i : \mathbb{N}^n \to \mathbb{N}^n\) such that

\[
\{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \vec{x} \in \text{REL}(\psi_i), \vec{x}' = A_i\vec{x} + \vec{b}_i\}
\]

- \(\text{REL}((A, \vec{b}, \psi))\) is equal to

\[
\{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : \exists \vec{y} \in \mathbb{N}^n f_1(\vec{x}) = \vec{y}, \vec{x} \in \text{dom}(f_1), f_2(\vec{y}) = \vec{x}', \vec{y} \in \text{dom}(f_2)\}
\]
Proof

- $\exists \vec{y} \in \mathbb{N}^n \ f_1(\vec{x}) = \vec{y}, \ \vec{x} \in \text{dom}(f_1), \ f_2(\vec{y}) = \vec{x}'$, $\vec{y} \in \text{dom}(f_2)$ is equivalent to the conditions:
  1. $\vec{x}' = A_2A_1\vec{x} + A_2\vec{b}_1 + \vec{b}_2$,
  2. $\vec{x} \in \text{REL}(\psi_1)$,
  3. $A_1\vec{x} + \vec{b}_1 \in \text{REL}(\psi_2)$.

- $A = A_2A_1$.

- $\vec{b} = A_2\vec{b}_1 + \vec{b}_2$.

- $\psi = \exists \vec{y} \ \psi_1(\vec{x}) \land (\vec{y} = A_1\vec{x} + \vec{b}_1) \land \psi_2(\vec{y})$ with
  - $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$.
  - $\vec{y} = A_1\vec{x} + \vec{b}_1$ is a shortcut for a conjunction made of $n$ conjuncts.
  - Indeed, each conjunct is of the form $y_i = \sum_j A(i, j)x_j + \vec{b}_1(i)$.  

- $\vec{b} = (b_1, \ldots, b_n)$.
Loop effect

\[(A, \vec{b}, \psi)\]

- How to represent symbolically
  \[X = \{(\vec{x}, \vec{x}') \in \mathbb{N}^{2n} : (q, \vec{x}) \mathrel{\rightarrow^*} (q, \vec{x}')\}?\]

- Is \(X\) definable in Presburger arithmetic?

- Reflexive and transitive closure \(R^* \subseteq \mathbb{N}^{2n}\) of \(R \subseteq \mathbb{N}^{2n}\):
  \[(\vec{y}, \vec{y}') \in R^* \iff \text{there are } \vec{x}_1, \ldots, \vec{x}_k \in \mathbb{N}^n \text{ such that}\]
  - \(\vec{x}_1 = \vec{y}\),
  - \(\vec{x}_k = \vec{y}'\),
  - for \(i \in [1, k - 1]\), we have \((\vec{x}_i, x_{i+1}) \in R\).
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 $\{ 2^\beta \in \mathbb{N} : \beta \in \mathbb{N} \}$.
  - Indeed, if $\text{REL}(\varphi(x, y)) = R^*$, then $\{ 2^\beta \in \mathbb{N} : \beta \in \mathbb{N} \} = \text{REL}(\varphi(x, y) \land x = 1)$.
  - Consequently, $R^*$ is not Presburger definable.
    (see next slide).

- 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.
$X = \{2^\beta : \beta \in \mathbb{N}\}$ is not semilinear

• Suppose that $X$ is semilinear.

• Since $X$ is infinite, there are $b \in \mathbb{N}$ and $p_1, \ldots, p_m > 0$ ($m \geq 1$) such that

$$Y = \{b + \sum_{i=1}^{i=m} n_ip_i : n_1, \ldots, n_m \in \mathbb{N}\} \subseteq X$$

• Let $2^\alpha \in Y$ such that $p_1 < 2^\alpha$.

• By definition of $Y$, we have $2^\alpha + p_1 \in Y$.

• However, $2^\alpha < 2^\alpha + p_1 < 2^{\alpha+1}$, which leads to a contradiction.
Presburger counting iteration

- The counting iteration of \( R \subseteq \mathbb{N}^{2n} \) is \( R_{\text{Cl}} \subseteq \mathbb{N}^n \times \mathbb{N} \times \mathbb{N}^n \) such that for all \( \vec{a}, i \) and \( \vec{b} \),

\[
(\vec{a}, i, \vec{b}) \in R_{\text{Cl}} \iff (\vec{a}, \vec{b}) \in R^i
\]

- \( R \) has a Presburger counting iteration \( \iff \) its counting iteration is Presburger definable.

- Assuming that \( R \) has a Presburger counting iteration:
  1. there is \( \chi(\vec{x}, z, \vec{y}) \) such that \( \text{REL}(\chi) = R_{\text{Cl}} \),
  2. \( \text{REL}(\exists z \chi) = R^* \).

- \( S = \{(\alpha, \alpha + 1) \in \mathbb{N}^2 : \alpha \in \mathbb{N} \} \) has a Presburger counter iteration but not \( \{(\alpha, 2\alpha) \in \mathbb{N}^2 : \alpha \in \mathbb{N} \} \).

- Exercise: compute \( \chi \) for \( S_{\text{Cl}} \).
Finite monoid property

- Let’s see a sufficient condition for having the Presburger counting iteration.

- For $A \in \mathbb{Z}^{n \times n}$, $A^*$ denotes the monoid generated from $A$ with $A^* = \{A^i : i \in \mathbb{N}\}$.

- In the monoid, the identity element is $A^0 = I$.

- With $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, we have

$$A^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad A^3 = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \quad \ldots$$

$$A^m = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$$
Finite monoid property and semilinearity

• Given $A \in \mathbb{Z}^{n \times n}$, checking whether the monoid generated by $A$ is finite, is decidable [Mandel & Simon, TCS 77].

• 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.
Proof – Preliminaries

• Let $R \subseteq \mathbb{N}^{2n}$ be defined by $(A, \vec{b}, \psi)$.

• $g$: affine update function obtained by ignoring the guard $\psi$.
  \[ g(\vec{a}) = A\vec{a} + \vec{b} \quad (g : \mathbb{Z}^n \to \mathbb{Z}^n) \]

• 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 ($k \geq 1$):
  • $g^k(\vec{a}) = A^k\vec{a} + A^{k-1}\vec{b} + \cdots + \vec{b}$ (easy induction on $k$).
  • $g^k(\vec{0}) = A^{k-1}\vec{b} + \cdots + \vec{b}$.  

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
  \[ A^k\vec{t} + A^{k-1}\vec{b} + \ldots + \vec{b} \]

- \( \psi(\vec{t}) \) is a shortcut for the Presburger formula
  \[ \exists x_1, \ldots, x_n \, \psi(x_1, \ldots, x_n) \land ( \bigwedge_{i \in [1, n]} x_i = \vec{t}(i)) \]
Proof – Quantifying over number of compositions

• For \( \vec{x}, \vec{x}' \in \mathbb{N}^n \), \( (\vec{x}, \vec{x}') \in R^* \) iff there is \( i \geq 0 \) such that
  1. \( \vec{x}' = g^i(\vec{x}) \),
  2. for \( 0 \leq j < i \), \( g^j(\vec{x}) \models \psi \), i.e. \( g^i(\vec{x}) \in \text{REL}(\psi) \).

• Presburger formula defining \( R^* \) may look like

\[
\exists i \ (\vec{x}' = g^i(\vec{x})) \land \bigwedge_{j<i} \psi(g^j(\vec{x})).
\]

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

• \( (\vec{x}' = g^i(\vec{x})) \land \bigwedge_{j<i} \psi(g^j(\vec{x})) \) 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 $g^{\alpha+q\beta}(\vec{a}) = g^\alpha(\vec{a}) + qA^\alpha g^\beta(\vec{0})$.

• $q$ as an exponent is transformed into a factor.

• $A^\alpha g^\beta(\vec{0})$ is constant tuple in $\mathbb{Z}^n$.

• For $i = \alpha + r + q\beta$ with $r < \beta$, 

\[
g^i(\vec{a}) = g^r(g^\alpha(\vec{a}) + qA^\alpha g^\beta(\vec{0})).
\]
\[(\text{Proof} – g^{\alpha + q\beta}(\vec{a}) = g^{\alpha}(\vec{a}) + qA^\alpha g^\beta(\vec{0}))\]

- Preliminary identities:

\[g^{\alpha + \beta}(\vec{a}) = A^{\alpha + \beta} \vec{a} + A^{\alpha + \beta - 1} \vec{b} + \cdots + \vec{b}.\]

\[= A^{\alpha + \beta} \vec{a} + A^{\alpha} (A^{\beta - 1} \vec{b} + \cdots + \vec{b}) + (A^{\alpha - 1} \vec{b} + \cdots + \vec{b})\]

\[= A^{\alpha} \vec{a} + A^{\alpha} g^\beta(\vec{0}) + (A^{\alpha - 1} \vec{b} + \cdots + \vec{b})\]

\[= g^{\alpha}(\vec{a}) + A^{\alpha} g^\beta(\vec{0}).\]

- Case \(q = 1\) is above.

- \(g^{\alpha + (q+1)\beta}(\vec{a}) = g^{\alpha}(g^\beta(\vec{a})) + qA^\alpha g^\beta(\vec{0})\) (by IH).

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

- \(g^{\alpha + (q+1)\beta}(\vec{a}) = g^{\alpha}(\vec{a}) + (q + 1)A^{\alpha} g^\beta(\vec{0}).\)
Proof – Towards the final formula

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

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

(free variables in $x_1, \ldots, x_n, x'_1, \ldots, x'_n$)

• $R[0]$ is equal to $\bigwedge_{j \in [1,n]} x_j = x'_j$.

• $R[i + 1]$ is equal to $\exists \vec{y} \psi(\vec{y}) \land R[i](\vec{x}, \vec{y}) \land (\vec{x}' = A\vec{y} + \vec{b})$.

• Again $\vec{x}' = A\vec{y} + \vec{b}$ is understood as a conjunction of $n$ conjuncts.

• To show that $R$ has a Presburger counting iteration, we define $\chi(\vec{x}, z, \vec{x}')$ such that $R_{\text{CI}} = \text{REL}(\chi(\vec{x}, z, \vec{x}'))$. 
A case analysis

- For $\vec{y}, \vec{y}' \in \mathbb{N}^n$, $(\vec{y}, \vec{y}') \in R^i$ for some $i$ iff for some $i$
  - $(\vec{y}, \vec{y}') \in R^i$,
  - for $0 \leq i' < i$, $g^{i'}(\vec{y}) \in \text{REL}(\psi)$ (guards satisfaction)
  - either $i < \alpha$ or $i = \alpha + r + q\beta$ with $r \in [0, \beta - 1]$, $q \in \mathbb{N}$ and $\vec{y}' = g^\alpha(\vec{y}) + qA^\alpha g^\beta(0)$.

- $\chi(\vec{x}, z, \vec{x}')$ shall be equal to:

$$
((z = 0 \land R[0]) \lor \cdots \lor (z = \alpha - 1 \land R[\alpha - 1])) \lor
(z \geq \alpha \land \exists q (\chi_{q,0} \lor \cdots \lor \chi_{q,\beta-1}))
$$

one formula per remainder $r$
Proof – Defining the last chunks

- $\chi_{q,r}$ is equal to $(z = \alpha + r + \beta \times q) \land$

$$\left( \exists \vec{y}' \ (\vec{y}' = A^\alpha \vec{x} + qA^\alpha (A^{\beta-1} \vec{b} + \cdots + \vec{b})) \land (\vec{x}' = g'(\vec{y}')) \right) \land \chi_{\text{guard}}(z, \vec{x})$$

- This encodes $g^i(\vec{a}) = g'(g^\alpha(\vec{a}) + qA^\alpha g^\beta(\vec{0}))$ and the point below.

- $\chi_{\text{guard}}(z, \vec{x})$ checks that the guard is satisfied for all the intermediate configurations.
\[ \chi^{\text{guard}}(z, \vec{x}) \overset{\text{def}}{=} \left( \bigwedge_{i \in [1, \alpha]} \exists \vec{y} \ R[i](\vec{x}, \vec{y}) \right) \land \forall z' \, \alpha \leq z' < z \Rightarrow \]

\[ \bigvee_{r' \in [1, \beta - 1]} \exists q' (z' = \alpha + r' + q' \beta) \land \exists \vec{y}' (\vec{y}' = A^\alpha \vec{x} + q' A^\alpha (A^{\beta-1} \vec{b} + \cdots + \vec{b})) \land \psi(g^{r'}(\vec{y}')) = g^{z'}(\vec{x}) \]
Admissible counter systems

- A loop in an affine counter system has the finite monoid property: \( A^* \) is finite for its corresponding affine update \((A, \vec{b}, \psi)\).

- Admissible counter system \( S \):
  1. \( S \) 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 $v$, we have $v \models \varphi$ iff $(q, (v(x_1), \ldots, v(x_n))) \xrightarrow{*} (q', (v(x'_1), \ldots, v(x'_n)))$.
  
  [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 $v_i \in \Sigma^+$. 
Encoding the effect of a path schema

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

- By closure under composition, for \( i \in [1, k + 1] \), there is a Presburger formula \( \psi^i_{\text{seg}}(\vec{x}, \vec{x}') \) that encodes the effect of segments of transitions \( u_i \).

- By previous theorem, for \( i \in [1, k] \), there is a Presburger formula \( \psi^i_{\text{loop}}(\vec{x}, z, \vec{x}') \) that encodes the effect of the loop \( v_i \).

- Presburger formula encoding the effect of the above sequence is the following (free variables in \( \vec{x}, \vec{x}' \)):

\[
\exists z_1, \ldots, z_k, \ y_1', \ y_2', \ y_2, \ldots, y_{k+1}'
\psi^1_{\text{seg}}(\vec{x}, \vec{y}_1') \land \psi^1_{\text{loop}}(\vec{y}_1', z_1, \vec{y}_2') \land \psi^2_{\text{seg}}(\vec{y}_2', z_1, \vec{y}_2) \land \psi^2_{\text{loop}}(\vec{y}_2', z_2, \vec{y}_3) \land \cdots \land \psi^k_{\text{loop}}(\vec{y}_k', z_k, y_{k+1}') \land \psi^{k+1}_{\text{seg}}(y_{k+1}', \vec{x}')
\]
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 $v$, we have

$$v \models \varphi \iff (q, (v(x_1), \ldots, v(x_n))) \xrightarrow{*} (q', (v(x'_1), \ldots, v(x'_n)))$$
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.
- \((S, (q, \vec{x}))\) is flattable whenever there is a partial unfolding of \((S, (q, \vec{x}))\) that is flat and has the same reachability set as \((S, (q, \vec{x}))\).
- \(\Sigma = \delta\); 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.
- \((S, (q, \vec{x}))\) is initially flattable \(\text{def}\) there is some \(L\) of the above form such that
  \[ \{(q', \vec{x}'): (q, \vec{x}) \xrightarrow{\ast} (q', \vec{x}')\} = \{(q', \vec{x}'): (q, \vec{x}) \xrightarrow{u} (q', \vec{x}'), u \in L\} \]
Is \((\mathcal{S}, (q_1, \vec{0}))\) initially fltable?
On being uniformly flattable

- $S$ is uniformly flattable $\iff$ there is a finite union of bounded languages $L$ such that
  
  $$\overset{*}{\rightarrow} = \{( (q, \bar{x}), (q', \bar{x}') ) : (q, \bar{x}) \xrightarrow{u} (q', \bar{x}'), u \in L \}$$

- Flattable counter systems are everywhere. [Leroux & Sutre, ATVA’05]
  
  - Uniformly reversal-bounded CA are uniformly flattable.
  
  - Reversal-bounded initialized CA are initially flattable.

- 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.
Conclusion

- Today’s lecture:
  - Reachability problems for reversal-bounded CA.
  - Affine counter systems with finite monoid property and flatness.
- Next lecture: Linear-time temporal logics on this class + exercises.
**Exo. 1**

1. Compute $\varphi(x_1, x_2, x'_1, x'_2)$ such that for every $v$, we have $v \models \varphi$ iff $(q_1, v(x_1), v(x_2)) \xrightarrow{*} (q_1, v(x'_1), v(x'_2))$.

2. Same question when $\top$ is replaced by $\neg(x_1 \equiv_{15} x_2)$. 

\[(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \top) \quad \text{and} \quad (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 \\ -3 \end{pmatrix}, x_1 < x_2)\]
1. Compute \( \varphi(x_1, x_2, z, x'_1, x'_2) \) such that for every \( \mathbf{v} \), we have \( \mathbf{v} \models \varphi \) iff on the unique run starting at \( (q_1, \mathbf{v}(x_1), \mathbf{v}(x_2)) \), the \( \mathbf{v}(z) \)th configuration has counter values \( (\mathbf{v}(x'_1), \mathbf{v}(x'_2)) \).

2. Given a Presburger formula \( \psi(y_1, y_2) \) viewed as a constraint on counter values, compute \( \varphi'(x_1, x_2) \) such that for every \( \mathbf{v} \), we have \( \mathbf{v} \models \varphi' \) iff on the unique run starting at \( (q_1, \mathbf{v}(x_1), \mathbf{v}(x_2)) \), the number of configurations with counter values satisfying \( \psi(y_1, y_2) \) is infinite.
Exo. 3

- Complete the undecidability proof for the $\exists$-PRESBURGER-ALWAYS PROBLEM.

- Update the definition of $S'$ by adding 4 counters such that the atomic formula $q_j$ above can be replaced by the Presburger formula $(x_7 - x_6 = j \land x_9 - x_8 = j)$.

- When succinct counter automata are considered, explain why 2 new counters suffice.