

Towards a model-checker for counter systems

S. Demri¹ A. Finkel¹ V. Goranko² G. van Drimmelen²

¹LSV, CNRS & ENS Cachan & INRIA Futurs

²University of Witwatersrand, Johannesburg

ATVA, October 2006, Beijing

Overview

Motivations

- Counter systems (CS)
- FAST success story

Presburger temporal logic

- Presburger counter systems
- Specification language
- Problems

Decision procedure

- Admissible CS
- Translation into PA

Procedure

- Flattening
- Completeness

Concluding remarks

Counter systems

- ▶ Model-checking of **infinite-state systems** needed for formal verification.
- ▶ **Ubiquity of counter systems (CS)**
 - ▶ Embedded systems/protocols, Petri nets, ...
 - ▶ Programs with pointer variables.
[Bardin et al, AVIS 06; Bouajjani et al, CAV 06]
 - ▶ Broadcast protocols. [Leroux & Finkel, FSTTCS 02]
 - ▶ Logics for data words. [Bojańczyk et al, LICS 06]
- ▶ **(High) undecidability**
 - ▶ Checking safety properties for CS is undecidable.
 - ▶ Checking liveness properties for CS is Σ_1^1 -hard.

Taming counter systems

▶ Classes with decidable reachability problems

- ▶ Reversal-bounded CS. [Ibarra, JACM 78]
- ▶ Flat relational CS. [Comon & Jurski, CAV 98]
- ▶ Flat linear CS. [Boigelot, PhD 98; Finkel & Leroux, FSTTCS 02]
- ▶ Petri nets. [Kosaraju, STOC 82]

▶ Verification techniques

- ▶ Acceleration method, ... [Boigelot & Wolper, CAV 94; Finkel & Leroux, FSTTCS 02]
- ▶ Flatness is central in the verification of CS. [Leroux & Sutre, ATVA 05; Bardin et al, ATVA 05]

▶ Tools: FAST, LASH, TReX, ...

FAST success story

- ▶ Verification of standard examples from Petri nets to TTP protocol and broadcast protocols.
- ▶ Cornerstones:
 - ▶ Flat CS with Presburger-definable reachability sets.
 - ▶ Homomorphisms between CS and flat CS preserving the reachability sets.
 - ▶ Complete procedure in FAST to enumerate flattenings.
- ▶ FAST Extended Release. [Bardin & Leroux & Point, CAV 06]

Our motivations

Theoretical ground to verify richer properties within FAST

- ▶ To design classes of counter systems with decidable temporal properties richer than reachability (à la CTL^{*}, ...).

Our motivations

Theoretical ground to verify richer properties within FAST

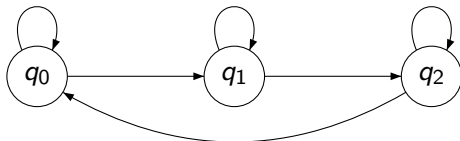
- ▶ To design classes of counter systems with decidable temporal properties richer than reachability (à la CTL*, ...).
- ▶ To provide the adequate notion of trace-flattening for such richer properties (preservation of traces, bisimulation, ...).

Our motivations

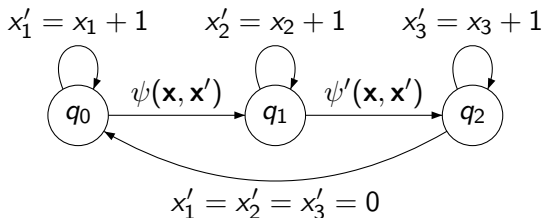
Theoretical ground to verify richer properties within FAST

- ▶ To design classes of counter systems with decidable temporal properties richer than reachability (à la CTL*, ...).
- ▶ To provide the adequate notion of trace-flattening for such richer properties (preservation of traces, bisimulation, ...).
- ▶ To design a procedure to enumerate trace-flattenings and then check the temporal properties.

Presburger counter systems (PCS) $\langle \Sigma, Q, T \rangle$



Presburger counter systems (PCS) $\langle \Sigma, Q, T \rangle$



- ▶ Labels: Presburger formulae over
 - ▶ $\mathbf{x} = \langle x_1, x_2, x_3 \rangle$ (current values).
 - ▶ $\mathbf{x}' = \langle x'_1, x'_2, x'_3 \rangle$ (next values).

Presburger transition systems (PTS)

$$\begin{array}{ccc}
 \text{Presburger CS} & \longrightarrow & \text{Presburger TS} \\
 \mathcal{C} = \langle \Sigma, Q, T \rangle & \mapsto & \mathcal{S}_{\mathcal{C}} = \langle S, \rightarrow \rangle
 \end{array}$$

- ▶ $S = Q \times \mathbb{N}^n$.
- ▶ $\langle q, \mathbf{a} \rangle \rightarrow \langle q', \mathbf{a}' \rangle$ iff $\exists q \xrightarrow{\psi(\mathbf{x}, \mathbf{x}')} q' \in T$ s.t. $\mathbf{a}, \mathbf{a}' \models \psi(\mathbf{x}, \mathbf{x}')$.
- ▶ Configuration path π : infinite path in $\langle S, \rightarrow \rangle$.

FOCTL*(Pr) formulae

$$\varphi ::= \overbrace{\psi(\mathbf{t})}^{Pr} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \overbrace{X\varphi \mid \varphi U \varphi \mid A\varphi}^{CTL^*} \mid \overbrace{\exists y \varphi}^{FO}.$$

► Variables:

x_0 : control state.

x_1, \dots, x_n : counters.

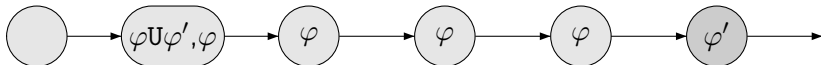
y, z, t, \dots : auxiliary variables.

► $\psi(\mathbf{t})$: Presburger formula with free variables from tuple \mathbf{t} .

Satisfaction relation

$$\pi, i \models_{env} \varphi$$

- ▶ π : infinite **configuration path** of some transition system S_C .



- ▶ i : **position** along π .
- ▶ env : **environment** $\text{VAR} \rightarrow \mathbb{N}$.
- ▶ φ : FOCTL^{*}(Pr) **formula**.

Main clauses of \models_{env}

- ▶ $\pi, i \models_{env} \psi(\mathbf{t})$ iff $\pi(i), env \models \psi(\mathbf{t})$ in PA,

Main clauses of \models_{env}

- ▶ $\pi, i \models_{env} \psi(\mathbf{t})$ iff $\pi(i), env \models \psi(\mathbf{t})$ in PA,
- ▶ $\pi, i \models X\varphi$ iff $\pi, i + 1 \models \varphi$,

Main clauses of \models_{env}

- ▶ $\pi, i \models_{env} \psi(\mathbf{t})$ iff $\pi(i), env \models \psi(\mathbf{t})$ in PA,
- ▶ $\pi, i \models \mathbf{X}\varphi$ iff $\pi, i + 1 \models \varphi$,
- ▶ $\pi, i \models_{env} \exists y\varphi$ iff there is $m \in \mathbb{N}$ such that $\pi, i \models_{env[y \leftarrow m]} \varphi$,

Main clauses of \models_{env}

- ▶ $\pi, i \models_{env} \psi(\mathbf{t})$ iff $\pi(i), env \models \psi(\mathbf{t})$ in PA,
- ▶ $\pi, i \models \mathbf{X}\varphi$ iff $\pi, i + 1 \models \varphi$,
- ▶ $\pi, i \models_{env} \exists y\varphi$ iff there is $m \in \mathbb{N}$ such that $\pi, i \models_{env[y \leftarrow m]} \varphi$,
- ▶ $\pi, i \models \varphi \mathbf{U} \varphi'$ iff there is some $j \geq i$ s.t. $\pi, j \models \varphi'$ and for $i \leq k < j$, we have $\pi, k \models \varphi$,
- ▶ $\pi, i \models \mathbf{A}\varphi$ iff for every infinite configuration path π' s.t. $\pi'_{\leq i} = \pi_{\leq i}$ we have $\pi', i \models \varphi$.

Examples of properties

Determinism : The reachability graph is deterministic:

$$\text{AG} \bigwedge_{0 \leq i \leq n} \neg \exists y (\text{EX}(x_i = y) \wedge \text{EX}(x_i \neq y)).$$

Examples of properties

Determinism : The reachability graph is deterministic:

$$\text{AG} \bigwedge_{0 \leq i \leq n} \neg \exists y (\text{EX}(x_i = y) \wedge \text{EX}(x_i \neq y)).$$

Boundedness : The reachability graph is finite:

$$\exists y \text{AG} \bigwedge_{1 \leq i \leq n} x_i \leq y.$$

Local model checking

▶ **input:**

- ▶ \mathcal{C} : PCS ; $\langle q, \mathbf{a} \rangle$: configuration
- ▶ φ : formula

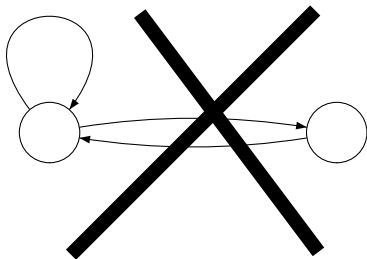
▶ **output:**

1 iff for every path π s.t. $\pi(0) = \langle q, \mathbf{a} \rangle$, we have $\pi, 0 \models \varphi$

Local MC is highly undecidable!

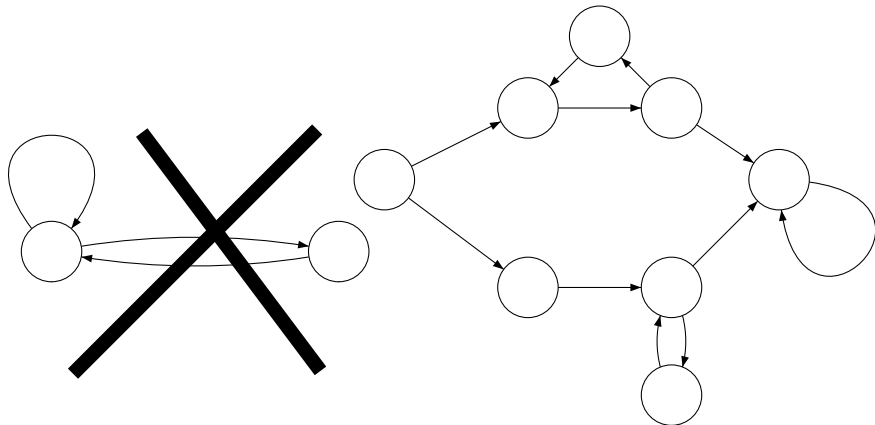
Flatness

A PCS is flat if every control state belongs to at most one cycle with no repeated vertex.



Flatness

A PCS is flat if every control state belongs to at most one cycle with no repeated vertex.



Functionality

- ▶ A PCS \mathcal{C} is functional iff every formula $\psi(\mathbf{x}, \mathbf{x}')$ labeling a transition in \mathcal{C} defines a partial function.
- ▶ It is decidable whether a given PCS is functional.
- ▶ The reachability problem is not decidable for all:
 - ▶ flat linear PCSs. [Cortier, TIA 02]
 - ▶ PCSs (Matrix = Id). [Minsky, 67]

Counting acceleration - Definitions

- ▶ $R \subseteq \mathbb{N}^n \times \mathbb{N}^n$.

$$\langle \mathbf{a}, i, \mathbf{b} \rangle \in R_{\mathbf{CA}} \text{ iff } \langle \mathbf{a}, \mathbf{b} \rangle \in R^i.$$

- ▶ R has Presburger counting acceleration (pca) iff $R_{\mathbf{CA}}$ is Presburger-definable.
- ▶ A PCS \mathcal{C} has pca iff every cycle relation in the control graph of \mathcal{C} has the pca.

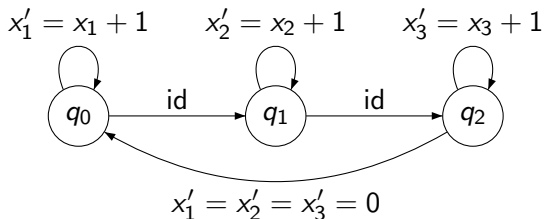
Admissible Presburger CS

Definition

A PCS is admissible if it is flat, functional, and has the pca.

- ▶ Reachability relation is Presburger-definable for flat PCS with pca, see e.g. [Finkel & Leroux, FSTTCS 02].
- ▶ Flatness and functionality are decidable properties.
- ▶ pca is conjectured undecidable, see [Leroux, TR LABRI 06].

An almost admissible PCS \mathcal{C}

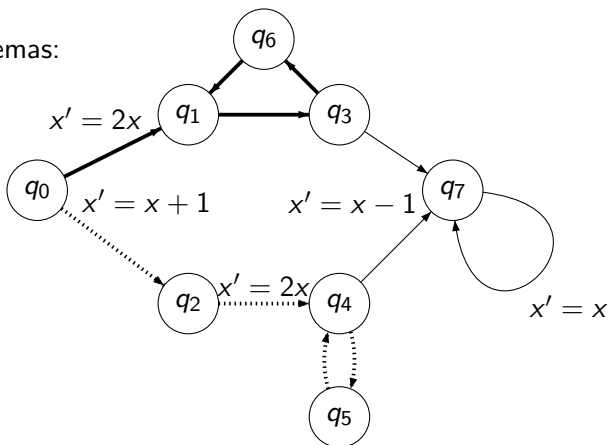


- ▶ The PCS \mathcal{C} is functional, has the pca but it is not flat.
- ▶ Local model-checking on \mathcal{C} with FOLTL*(Pr) is Σ_1^1 -hard.

Encoding configuration paths in Presburger arithmetic

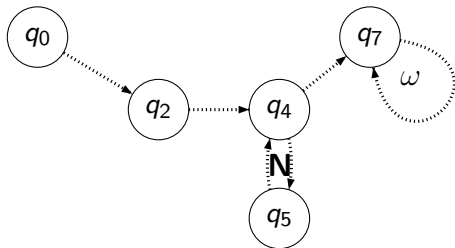
- ▶ Control path: infinite control path in \mathcal{C} .

- ▶ Path schemas:



Control path description

- ▶ Control path description: path schema + counters for cycles.



For admissible PCS,

- ▶ every control path has a unique control path description.
- ▶ a configuration path is determined by
a control path description + an initial configuration.

Local MC is Presburger-definable

- ▶ Admissible PCS \mathcal{C} and FOCTL*(Pr) formula φ . One can compute a Presburger formula $\psi(\mathbf{x})$ such that for every configuration $\langle q, \mathbf{a} \rangle$,

$$\langle q, \mathbf{a} \rangle \models \psi(\mathbf{x}) \text{ iff } \mathcal{C}, \langle q, \mathbf{a} \rangle \models \varphi.$$

- ▶ Local model-checking over admissible PCS for FOCTL*(Pr) is decidable.
- ▶ Decidable extensions:
 - ▶ Past-time operators S, X^{-1} .
 - ▶ CQDD-based temporal operators à la Wolper.

Flattening [Bardin et al, ATVA 05]

Let $\mathcal{C} = \langle \Sigma, Q, T \rangle$ and $\mathcal{C}' = \langle \Sigma, Q', T' \rangle$ be PCSs, $f : Q' \rightarrow Q$.

$\langle \mathcal{C}', q' \rangle$ is a f -flattening of $\langle \mathcal{C}, q \rangle$ iff

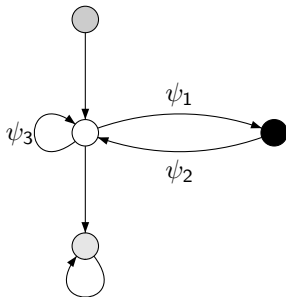
- ▶ $f(q') = q$,
- ▶ \mathcal{C}' is flat,
- ▶ $r \xrightarrow{\psi(\mathbf{x}, \mathbf{x}')} s \in T'$ implies $f(r) \xrightarrow{\psi(\mathbf{x}, \mathbf{x}')} f(s) \in T$.

A flattable non flat PCS

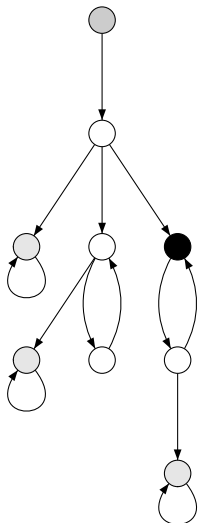
$$\psi_1 \stackrel{\text{def}}{=} x \neq 1 \wedge \psi$$

$$\psi_2 \stackrel{\text{def}}{=} x' = 0 \wedge \psi'$$

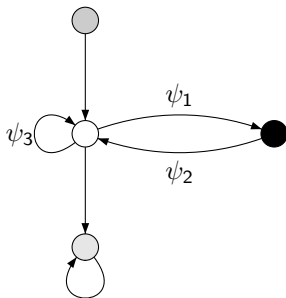
$$\psi_3 \stackrel{\text{def}}{=} x \neq 0 \wedge x' = 1 \wedge \psi''$$



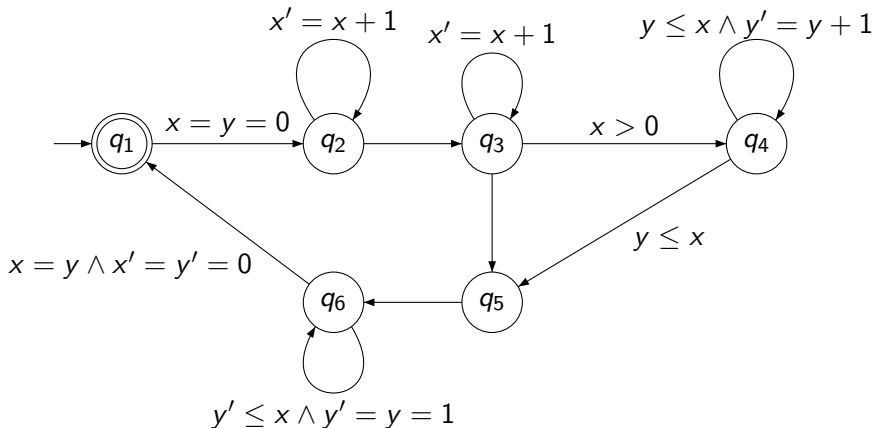
A flattable non flat PCS



$$\begin{aligned} \psi_1 &\stackrel{\text{def}}{=} x \neq 1 \wedge \psi \\ \psi_2 &\stackrel{\text{def}}{=} x' = 0 \wedge \psi' \\ \psi_3 &\stackrel{\text{def}}{=} x \neq 0 \wedge x' = 1 \wedge \psi'' \end{aligned}$$



Another flattable non flat PCS



Trace-flattening

- ▶ $\langle \mathcal{C}', q' \rangle$ is a f -trace-flattening of $\langle \mathcal{C}, q \rangle$ wrt $\psi(\mathbf{x})$ iff
 - ▶ $\langle \mathcal{C}', q' \rangle$ is a f -flattening of $\langle \mathcal{C}, q \rangle$.
 - ▶ Preservation of sets of traces:

$$\text{traces}_{\mathcal{C}}(q, \psi(\mathbf{x})) = f(\text{traces}_{\mathcal{C}'}(q', \psi(\mathbf{x}))).$$

- ▶ $\langle \mathcal{C}', q' \rangle$ f -flattening of $\langle \mathcal{C}, q \rangle$ and \mathcal{C}' admissible. It is decidable whether $\langle \mathcal{C}', q' \rangle$ is a trace-flattening of $\langle \mathcal{C}, q \rangle$ wrt $\psi(\mathbf{x})$.
- ▶ $\langle \mathcal{C}', q' \rangle$ trace-flattening of $\langle \mathcal{C}, q \rangle$ wrt \mathbf{a} .

$$\mathcal{C}', \langle q', \mathbf{a} \rangle \models \varphi \text{ iff } \mathcal{C}, \langle q, \mathbf{a} \rangle \models \varphi,$$

for any φ from the LTL fragment.

Model-checking(\mathcal{C} : funct. PCS + pca; φ : FOLTL(Pr))

procedure model-check(\mathcal{C} , $\langle q, \mathbf{a} \rangle$, φ)

1. *found* := *false*;
2. **while** not *found* **do**
 - 2.1 Choose fairly a flattening $\langle \mathcal{C}', q' \rangle$ of $\langle \mathcal{C}, q \rangle$;
 - 2.2 **if** $\langle \mathcal{C}', q' \rangle$ is a trace-flattening of $\langle \mathcal{C}, q \rangle$ **then** *found* := *true*;
3. **return** $\mathcal{C}', \langle q', \mathbf{a} \rangle \models \varphi$.

Completeness

Theorem

- (I) *model-check($\mathcal{C}, \langle q, \mathbf{a} \rangle, \varphi$) terminates iff $\langle \mathcal{C}, q \rangle$ has a trace-flattening wrt to $\langle q, \mathbf{a} \rangle$.*
- (II) *When model-check($\mathcal{C}, \langle q, \mathbf{a} \rangle, \varphi$) terminates, it returns whether $\mathcal{C}, \langle q, \mathbf{a} \rangle \models \varphi$ holds true.*

Conclusion

- ▶ Procedure to verify first-order LTL properties over trace-flattable CSs.
- ▶ Decidability of model-checking $\text{FOCTL}^*(\text{Pr})$ over admissible CSs.
- ▶ Open problems:
 - ▶ Extension to bisimulation-flattening (preserving CTL^* properties)?
 - ▶ What are the trace-flattable systems in the literature?
 - ▶ Decidability status of model-checking “Presburger mu-calculus” over admissible PCS?
 - ▶ Complexity of local model checking admissible PCS over $\text{FOCTL}^*(\text{Pr})$ when each $\psi(\mathbf{x}, \mathbf{x}')$ is quantifier-free?