Presburger Arithmetic
Reversal-Bounded Counter Machines

Stéphane Demri (demri@lsv.fr)

October 16th, 2015

Slides and lecture notes

http://www.lsv.fr/~demri/notes-de-cours.html

https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:c-2-9-1

Plan of the lecture

- Previous lecture :
  - Introduction to Presburger arithmetic.
  - Decidability and quantifier elimination.
  - Automata-based approach.

- Presburger sets are the semilinear sets.
- Application: Parikh image of regular languages.
- Introduction to reversal-bounded counter machines.
- Runs in normal form.

The previous lecture in 2 slides (1/2)

- First-order theory $\mathrm{FO}(\mathbb{N})$ on $\langle \mathbb{N}, \leq, + \rangle$:

$$\varphi ::= \top \mid \perp \mid t \leq t' \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists \mathsf{x}\ \varphi \mid \forall \mathsf{x}\ \varphi$$

- Presburger sets

$$[\![\varphi(\mathsf{x}_1, \ldots, \mathsf{x}_n)]\!] \stackrel{\text{def}}{=} \{\langle \mathfrak{v}(\mathsf{x}_1), \ldots, \mathfrak{v}(\mathsf{x}_n)\rangle \in \mathbb{N}^n : \mathfrak{v} \models \varphi\}$$

- Quantifier-free fragment

$$\top \mid \perp \mid t \leq t' \mid t \equiv_k t' \mid t = t' \mid t < t' \mid t \geq t' \mid t > t'$$

- The satisfiability problem for the quantifier-free fragment is NP-complete.

Previous lecture in 2 slides (2/2)

- For every φ, there is a quantifier-free formula φ' such that
  1. $\mathit{free}(\varphi') \subseteq \mathit{free}(\varphi)$.
  2. φ' is logically equivalent to φ.
  3. φ' can be effectively built from φ.
- Presburger arithmetic is decidable.
- Alternative proof with the automata-based approach:
  "Presburger sets as regular languages of finite words"

Semilinear Sets

Formulae with one free variable

$$\varphi(\mathsf{x}) \stackrel{\text{def}}{=} (\mathsf{x} \neq 1 \wedge \mathsf{x} \neq 2) \wedge (\mathsf{x} = 0 \vee (\mathsf{x} \geq 3 \wedge \exists\, \mathsf{y}\ (\mathsf{x} = 3 + 2\mathsf{y})))$$

$$[\![\varphi(\mathsf{x})]\!] = \{0\} \cup \{3 + 2n : n \geq 0\}$$

- After the value 3, every two value belongs to $[\![\varphi(\mathsf{x})]\!]$.

$$\bullet \circ \circ \bullet \circ \bullet \circ \bullet \circ \bullet \circ \bullet \circ \bullet \circ \bullet \ldots$$

- This can be generalized.

$X \subseteq \mathbb{N}$ is ultimately periodic

$\stackrel{\text{def}}{\Leftrightarrow}$

there exist $N \geq 0$ and $P \geq 1$ such that for all $n \geq N$, we have $n \in X$ iff $n + P \in X$.

$$\overbrace{\bullet \circ \circ \bullet \circ \bullet \circ}^{N \text{ first values}} \quad \overbrace{\bullet \bullet \circ \bullet \bullet}^{\text{period of length } P} \quad \bullet \bullet \circ \bullet \bullet \bullet \bullet \circ \bullet \bullet \bullet \bullet \circ \bullet \bullet \ldots$$

Examples of ultimately periodic sets

- The set of even numbers is ultimately periodic (with $N = 0$ and $P = 2$).
- The set of odd numbers is ultimately periodic (with $N = 1$ and $P = 2$).
- $[\![\mathrm{x} \equiv_k k']\!]$ is ultimately periodic (with $N = 0$ and $P = k$).
- Ultimately periodic sets are closed under union, intersection and complementation.

Proof for complementation

- Suppose X is ultimately periodic and $\overline{X} = \mathbb{N} \setminus X$.
- The statements below are equivalent for $n \geq N$:
  - $n \in \overline{X}$,
  - $n \notin X$
    (by definition of $\overline{X}$),
  - $n + P \notin X$
    (X is ultimately periodic with parameters N and P),
  - $n + P \in \overline{X}$
    (by definition of $\overline{X}$).
- $\overline{X}$ is ultimately periodic too and the same parameters N and P can be used.

● ○ ○ ● ○ ● ○ ● ● ○ ● ● ● ● ○ ● ● ● ● ○ ● ● ● ● ○ ● ● . . .

○ ● ● ○ ● ○ ● ○ ○ ● ○ ○ ○ ○ ● ○ ○ ○ ○ ● ○ ○ ○ ○ ● ○ ○ . . .

Ultimately periodic sets X are Presburger sets

$$(\bigwedge_{k\in[0,N-1]\setminus X} \mathsf{x}\neq k)\wedge[(\bigvee_{k\in[0,N-1]\cap X} \mathsf{x}=k)\vee$$

$$((\mathsf{x}\geq N)\wedge(\exists\, \mathsf{y} \bigvee_{k\in[N,N+P-1]\cap X}(\mathsf{x}=k+P\mathsf{y})))]$$

It remains to show the converse result.

Semilinear sets of dimension 1

For every formula $\varphi(x)$ with a unique free variable x, $[\![\varphi]\!]$ is an ultimately periodic set.

- Formula $\varphi(x)$ with a unique free variable x.
- φ': equivalent quantifier-free formula.
- φ' is a Boolean combination of atomic formulae of one of the forms below: $\top$, $\bot$, $x \leq k$, $x \equiv_k k'$.
- Each atomic formula defines an ultimately periodic set and ultimately periodic sets are closed under union, intersection and complementation.
- So $[\![\varphi']\!] = [\![\varphi]\!]$ is ultimately periodic.

Semilinear sets

- A linear set X is defined by a basis $\mathbf{b} \in \mathbb{N}^d$ and a finite set of periods $\mathfrak{P} = \{\mathbf{p}_1, \ldots, \mathbf{p}_m\} \subseteq \mathbb{N}^d$:

$$X = \{\mathbf{b} + \sum_{i=1}^{i=m} n_i \mathbf{p}_i : n_1, \ldots, n_m \in \mathbb{N}\}$$

- A linear set:

$$\left\{ \begin{pmatrix} 3 \\ 4 \end{pmatrix} + i \times \begin{pmatrix} 2 \\ 5 \end{pmatrix} + j \times \begin{pmatrix} 4 \\ 7 \end{pmatrix} : i, j \in \mathbb{N} \right\}$$

- A semilinear set is a $\boxed{\text{finite}}$ union of linear sets.

- Each semilinear set can be represented by a finite set of pairs of the form $\langle \mathbf{b}, \mathfrak{P} \rangle$.

Ultimately periodic sets are semilinear sets

- Ultimately periodic set X with parameters N and P.

$$X = \Big(\bigcup_{n \in [0, N-1] \cap X} \{n\}\Big) \cup \Big(\bigcup_{n \in [N, N+P-1] \cap X} \{n + \lambda P : \lambda \in \mathbb{N}\}\Big)$$

- $\{n\}$ is a linear set with no period.
- $\{n + \lambda P : \lambda \in \mathbb{N}\}$ is a linear set with basis n and unique period P.

The fundamental characterisation

[Ginsburg & Spanier, PJM 66]

- For every Presburger formula φ with $d \geq 1$ free variables, $[\![\varphi]\!]$ is a semilinear subset of $\mathbb{N}^d$.
- For every semilinear set $X \subseteq \mathbb{N}^d$, there is φ such that $X = [\![\varphi]\!]$.
- The class of semilinear sets are effectively closed under union, intersection, complementation and projection.
- For instance, ($X_1 = [\![\varphi_1]\!]$ and $X_2 = [\![\varphi_2]\!]$) imply $X_1 \cap X_2 = [\![\varphi_1 \wedge \varphi_2]\!]$
- Presburger formula for

$$\left\{ \begin{pmatrix} 3 \\ 4 \end{pmatrix} + i \times \begin{pmatrix} 2 \\ 5 \end{pmatrix} + j \times \begin{pmatrix} 4 \\ 7 \end{pmatrix} : i, j \in \mathbb{N} \right\}$$

$$\exists \, \mathsf{y}, \mathsf{y}' \, (\mathsf{x}_1 = 3 + 2\mathsf{y} + 4\mathsf{y}' \wedge \mathsf{x}_2 = 4 + 5\mathsf{y} + 7\mathsf{y}')$$

$X = \{2^n : n \in \mathbb{N}\}$ is not a Presburger set

- *Ad absurdum*, suppose that X is semilinear.
- Since X is infinite, there are $\mathbf{b} \geq 0$ and $\mathbf{p}_1, \ldots, \mathbf{p}_m > 0$ ($m \geq 1$) such that

$$Y \stackrel{\text{def}}{=} \{\mathbf{b} + \sum_{i=1}^{m} \lambda_i \mathbf{p}_i : \lambda_1, \ldots, \lambda_m \in \mathbb{N}\} \subseteq X$$

- There exists $2^\alpha \in Y$ such that $\mathbf{p}_1 < 2^\alpha$.
- By definition of Y, we have $2^\alpha + \mathbf{p}_1 \in Y$.
- But, $2^\alpha < 2^\alpha + \mathbf{p}_1 < 2^{\alpha+1}$, contradiction.

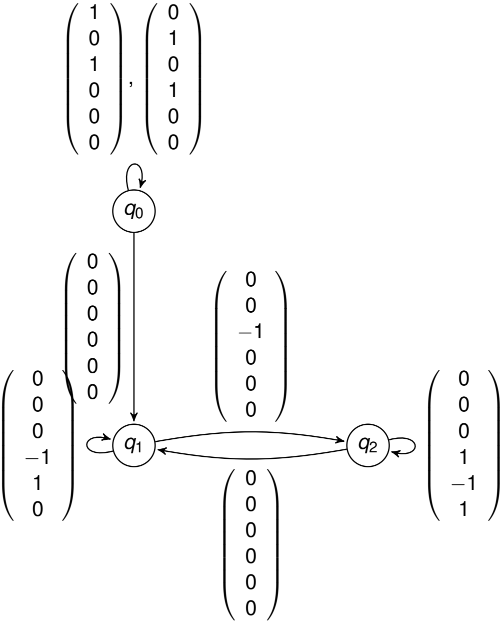
$X = \{n^2 : n \in \mathbb{N}\}$ is not a Presburger set

- *Ad absurdum*, suppose that X is semilinear.
- Since X is infinite, there are $\mathbf{b} \geq 0$ and $\mathbf{p}_1, \ldots, \mathbf{p}_m > 0$ ($m \geq 1$) such that

$$Z \stackrel{\text{def}}{=} \{\mathbf{b} + \sum_{i=1}^{m} \lambda_i \mathbf{p}_i : \lambda_1, \ldots, \lambda_m \in \mathbb{N}\} \subseteq X$$

- Let $N \in \mathbb{N}$ be such that $N^2 \in Z$ and $(2N + 1) > \mathbf{p}_1$.
- Since Z is a linear set, we also have $(N^2 + \mathbf{p}_1) \in Z$.
- However $(N + 1)^2 - N^2 = (2N + 1) > \mathbf{p}_1$.
- Hence $N^2 < N^2 + \mathbf{p}_1 < (N + 1)^2$, contradiction.

A VASS weakly computing multiplication



Weak multiplication

$$\left\{ \begin{pmatrix} a \\ b \\ f \end{pmatrix} \in \mathbb{N}^3 \;\middle|\; \exists \begin{pmatrix} c \\ d \\ e \end{pmatrix} \in \mathbb{N}^3,\ \langle q_0, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rangle \xrightarrow{*} \langle q_1, \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} \rangle \right\} =$$

$$\left\{ \begin{pmatrix} n \\ m \\ p \end{pmatrix} \in \mathbb{N}^3 : p \leq n \times m \right\}.$$

Weak multiplication in a VASS

- Suppose there is $\varphi(x_1, \ldots, x_6)$ such that

$$[\![\varphi(x_1, \ldots, x_6)]\!] = \left\{ \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} \;\middle|\; \langle q_0, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rangle \xrightarrow{*} \langle q_1, \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} \rangle \right\}$$

- Formula $\psi(x)$ below verifies $[\![\psi(x)]\!] = \{n^2 \mid n \in \mathbb{N}\}$

$$\exists\, x_1, \ldots, x_5\; \varphi(x_1, \ldots, x_5, x) \wedge x_1 = x_2 \wedge$$

$$\forall\, x'\; (x' > x) \Rightarrow \neg\exists\, x_3, x_4, x_5\; \varphi(x_1, \ldots, x_5, x')$$

Contradiction!

Parikh Image of Regular Languages

Parikh image

- $\Sigma = \{a_1, \ldots, a_k\}$ with ordering $a_1 < \cdots < a_k$.
- Parikh image of $u \in \Sigma^*$: $\begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} \in \mathbb{N}^k$ where each n_j is the number of occurrences of a_j in u.
- Parikh image of $a\ b\ a\ a\ b$ is $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$.
- Definition for Parikh image extends to languages.
- The Parikh image of any context-free language is semilinear. [Parikh, JACM 66]
- Effective computation from pushdown automata.

Bounded languages

- Language $\mathrm{L} \subseteq \Sigma^*$ bounded $\overset{\text{def}}{\Leftrightarrow}$

  $$\mathrm{L} \subseteq u_1^* \cdots u_n^*$$

  for some words $u_1, \ldots, u_n$ in Σ^*.

- $\mathrm{L} \subseteq \Sigma^*$ is bounded and regular iff it is a finite union of languages of the form

  $$u_0 v_1^* u_1 \cdots v_k^* u_k$$

- The Parikh images of bounded and regular languages are semilinear (i.e. Presburger sets).

Counting letters in bounded and regular languages

- Parikh image of $u_0 v_1^* u_1 \cdots v_k^* u_k$ is equal to

$$\{\mathbf{b} + \lambda_1 \mathbf{p}_1 + \cdots \lambda_k \mathbf{p}_k : \lambda_1, \ldots, \lambda_k \in \mathbb{N}\}$$

  with
  - $\mathbf{b} = \Pi(u_0) + \cdots + \Pi(u_k)$,
  - $\mathbf{p}_i = \Pi(v_i)$ for every $i \in [1, k]$.
- Finite union of such languages handled by finite unions of linear sets.
- Then, contructing a Presburger formula for the Parikh image easily follows.

Underapproximation by bounded languages

- For every regular language L, there is a bounded and regular language L' such that
  1. $\mathrm{L}' \subseteq \mathrm{L}$,
  2. $\Pi(\mathrm{L}') = \Pi(\mathrm{L})$.
- The proof consists in constructing effectively the bounded language L'.
- $\mathcal{A} = \langle \Sigma, Q, Q_0, \delta, F \rangle$ such that $\mathrm{Lan}(\mathcal{A}) = \mathrm{L}$.
- W.l.o.g., $Q_0 \cap F \neq \emptyset$ (otherwise add ε to the bounded language).

Paths, simple loops and extended paths

- Path π: finite sequence of transitions corresponding to a path in the control graph of $\mathcal{A}$.
- $\mathrm{first}(\pi)$ [resp. $\mathrm{last}(\pi)$]: first [resp. last] state of a path π.
- *lab*(π): label of π as a word of Σ^*.
- Simple loop *sl*: non-empty path that starts and ends by the same state and this is the only repeated state in it.
- "*sl* loops on its first state".
- Number of simple loops $\leq \mathrm{card}(\delta)^{\mathrm{card}(Q)}$.
- Arbitrary total linear ordering $\prec$ on simple loops.

Generalising the notion of path

- Encoding families of paths with extended paths.
- Extended path **P**:

$$\pi_0 \; S_1 \; \pi_1 \; \cdots \; S_\alpha \; \pi_\alpha$$

1. the S_i's are non-empty sets of simple loops,
2. the π_i's are non-empty paths,
3. if S occurs just before [resp. after] a path π, then all the simple loops in S loops on the first [resp. last] state of π.

Some more auxiliary notions

- Skeleton of **P** is the path $\pi_0 \cdots \pi_\alpha$.
- $S = \{sl_1, \ldots, sl_m\}$ with $sl_1 \prec \cdots \prec sl_m$

$$e(S) \stackrel{\text{def}}{=} lab(sl_1)^+ \cdots lab(sl_m)^+$$

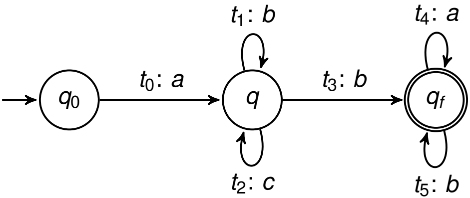
- $e(\mathbf{P}) \stackrel{\text{def}}{=} lab(\pi_0) \cdot e(S_1) \cdots e(S_\alpha) \cdot lab(\pi_\alpha)$.
- $\mathrm{Lan}(e)$: language defined by the regular expression e.
- $\mathrm{Lan}(\mathbf{P}) \stackrel{\text{def}}{=} \mathrm{Lan}(e(\mathbf{P}))$.
- When the first state occuring in the skeleton of **P** is in Q_0 and the last state is in F, then

$$\mathrm{Lan}(e(\mathbf{P})) \subseteq \mathrm{Lan}(\mathcal{A})$$

Small extended path

- Small extended path:
  1. π_0 and π_α have at most $2 \times \mathrm{card}(Q)$ transitions,
  2. $\pi_1, \ldots, \pi_{\alpha-1}$ have at most $\mathrm{card}(Q)$ transitions,
  3. for each $q \in Q$, there is at most one set S containing simple loops on q.
- Length of the skeleton bounded by $\mathrm{card}(Q)(3 + \mathrm{card}(Q))$.
- The set of small extended paths is finite.

Example



- Small extended path **P**

$$t_0 \cdot t_1 \cdot \{t_1, t_2\} \cdot t_3 \cdot \{t_4, t_5\} \cdot t_4 \cdot t_5 \cdot t_5$$

- Regular expression $e(\mathbf{P})$ (with $t_1 \prec t_2$ and $t_5 \prec t_4$)

$$a \cdot b \cdot b^+ \cdot c^+ \cdot b \cdot b^+ \cdot a^+ \cdot a \cdot b \cdot b$$

How to proceed from a given run ρ

- Sequence of accepting extended paths $\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_\beta$ such that
  - all the $\mathbf{P}_i$'s are accepting extended paths,
  - $\mathbf{P}_0$ is equal to ρ viewed as an extended path,
  - $\mathbf{P}_\beta$ is a small and accepting extended path,
  - $\mathbf{P}_{i+1}$ is obtained from $\mathbf{P}_i$ by removing a simple loop while $\Pi(\mathrm{Lan}(\mathbf{P}_i)) \subseteq \Pi(\mathrm{Lan}(\mathbf{P}_{i+1}))$.
- At the end of this process,

$$\Pi(\mathit{lab}(\rho)) \in \Pi(\mathrm{Lan}(\mathbf{P}_\beta)) \quad \text{and} \quad \Pi(\mathrm{Lan}(\mathbf{P}_\beta)) \subseteq \Pi(\mathrm{Lan}(\mathcal{A}))$$

From $\mathbf{P}_i$ to $\mathbf{P}_{i+1}$

$$\mathbf{P}_i = \pi_0 \; S_1 \; \pi_1 \; \cdots \; S_\alpha \; \pi_\alpha$$

(a) $\alpha \leq \mathrm{card}(Q)$,

(b) each path in $\pi_1, \ldots, \pi_{\alpha-1}$ have length less than $\mathrm{card}(Q)$,

(c) each state has at most one S_i with simple loops on it.

$\mathbf{P}_0$ verifies these conditions.

Three cases (1/2)

- $\mathbf{P}_i$ is a small extended path. We are done.

- $\pi_\alpha = \pi \cdot sl \cdot \pi'$ where
  1. sl is a simple loop on q,
  2. $\pi\pi' \neq \varepsilon$,
  3. S_γ already contains simple loops on q.

  $\mathbf{P}_{i+1}$ is equal to:

$$\pi_0 \ \cdots \ S_{\gamma-1} \ \pi_{\gamma-1} \ (S_\gamma \cup \{sl\}) \ \cdots \ \pi_{\alpha-1} \ S_\alpha \ (\pi\pi')$$

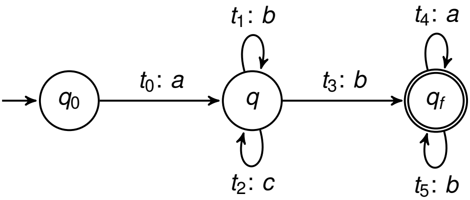
Three cases (2/2)

- $\pi_\alpha = \pi \cdot sl \cdot \pi'$ where
  1. sl is a simple loop on q,
  2. the first one occurring in $\pi \cdot sl$,
  3. $\pi\pi' \neq \varepsilon$,
  4. no S_γ already contains simple loops on q.

  $\mathbf{P}_{i+1}$ is equal to: $\pi_0 \; \cdots \; S_\alpha \; \pi \; \{sl\} \; \pi'$.

- Three properties easy to prove:
  1. $\Pi(\mathrm{Lan}(\mathbf{P}_i)) \subseteq \Pi(\mathrm{Lan}(\mathbf{P}_{i+1}))$.
  2. $\mathbf{P}_{i+1}$ satisfies the three previous conditions.
  3. $\mathrm{Lan}(\mathbf{P}_{i+1}) \subseteq \mathrm{Lan}(\mathcal{A})$.

Example



$$t_0 \cdot (t_1)^7 \cdot (t_2)^7 (t_1)^8 \cdot t_3 \cdot (t_4)^7 \cdot (t_5)^7 \cdot (t_4)^8$$

- $\mathbf{P}_{22} = t_0 \cdot \{t_1, t_2\} \cdot t_3 \cdot (t_4)^7 \cdot (t_5)^7 \cdot (t_4)^8$.
- $\mathbf{P}_{38} = t_0 \cdot \{t_1, t_2\} \cdot t_3 \cdot \{t_4, t_5\} \cdot (t_4)^6$.
- $\mathbf{P}_{38}$ is a small extended path.

Time to conclude!

- FSA $\mathcal{A}$ over a k-size alphabet Σ. One can compute a formula $\varphi_{\mathcal{A}}(\mathsf{x}_1, \ldots, \mathsf{x}_k)$ in $\mathrm{FO}(\mathbb{N})$ such that

$$\Pi(\mathrm{Lan}(\mathcal{A})) = [\![\varphi_{\mathcal{A}}]\!]$$

- $\mathrm{Lan}(\mathcal{A})$ includes a bounded and regular language L with the same Parikh image.

- L can be computed by enumerating the regular expressions obtained from small and accepting extended paths and then check inclusion with $\mathrm{Lan}(\mathcal{A})$.

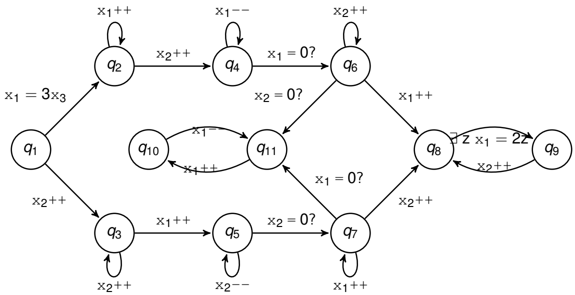
- Disjunction made of the formulae obtained for each bounded and regular language included in $\mathrm{Lan}(\mathcal{A})$.

- When $Q_0 \cap F \neq \emptyset$, we include a disjunct stating that all the values are equal to zero.

Presburger Counter Machines

Presburger counter machines (PCM)

- Presburger counter machine $\mathcal{M} = \langle Q, T, C \rangle$:
  - Q is a nonempty finite set of control states.
  - C is a finite set of counters $\{\mathrm{x}_1, \ldots, \mathrm{x}_d\}$ for some $d \geq 1$.
  - T = finite set of transitions of the form $t = \langle q, \varphi, q' \rangle$ where $q, q' \in Q$ and φ is a Presburger formula with free variables $\mathrm{x}_1, \ldots, \mathrm{x}_d, \mathrm{x}'_1, \ldots, \mathrm{x}'_d$.

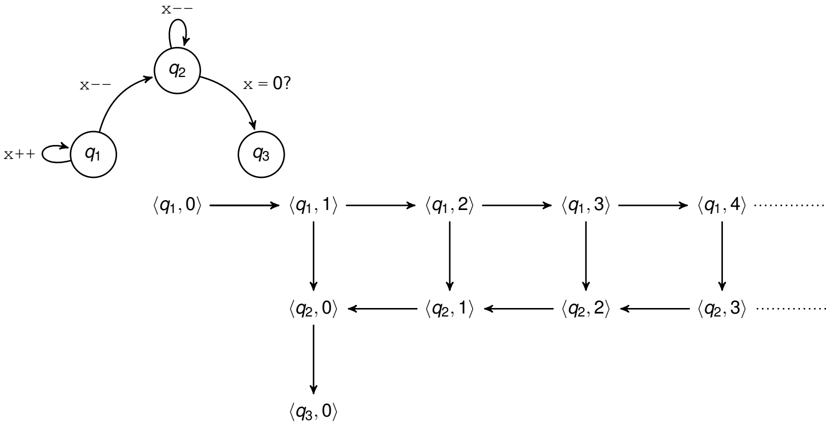


- Configuration $\langle q, \mathbf{x} \rangle \in Q \times \mathbb{N}^d$.

Transition system $\mathfrak{T}(\mathcal{M})$

- Transition system $\mathfrak{T}(\mathcal{M}) = \langle Q \times \mathbb{N}^d, \rightarrow \rangle$:

$$\langle q, \mathbf{x} \rangle \rightarrow \langle q', \mathbf{x}' \rangle \quad \overset{\text{def}}{\Leftrightarrow} \quad \text{there is } t = \langle q, \varphi, q' \rangle \text{ s.t. } \mathfrak{v}[\overline{\mathtt{x}} \leftarrow \mathbf{x}, \overline{\mathtt{x}'} \leftarrow \mathbf{x}'] \models \varphi$$



- $\xrightarrow{*}$: reflexive and transitive closure of $\rightarrow$.

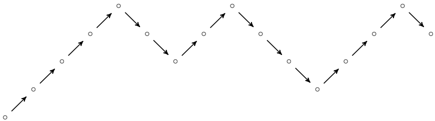
Decision problems

- Reachability problem:
  - Input: PCM $\mathcal{M}$, $\langle q_0, \mathbf{x}_0 \rangle$ and $\langle q_f, \mathbf{x}_f \rangle$.
  - Question: $\langle q_0, \mathbf{x}_0 \rangle \xrightarrow{*} \langle q_f, \mathbf{x}_f \rangle$?
- Control state reachability problem:
  - Input: PCM $\mathcal{M}$, $\langle q_0, \mathbf{x}_0 \rangle$ and q_f.
  - Question: $\exists \mathbf{x}_f \ \langle q_0, \mathbf{x}_0 \rangle \xrightarrow{*} \langle q_f, \mathbf{x}_f \rangle$?
- Control state repeated reachability problem:
  - Input: PCM $\mathcal{M}$, $\langle q_0, \mathbf{x}_0 \rangle$ and q_f.
  - Question: is there an infinite run starting from $\langle q_0, \mathbf{x}_0 \rangle$ such that the control state q_f is repeated infinitely often?
- Boundedness problem:
  - Input: PCM $\mathcal{M}$ and $\langle q_0, \mathbf{x}_0 \rangle$.
  - Question: is the set of configurations reachable from $\langle q_0, \mathbf{x}_0 \rangle$ finite?

What is Reversal-Boundedness?

Reversal-bounded counter machines

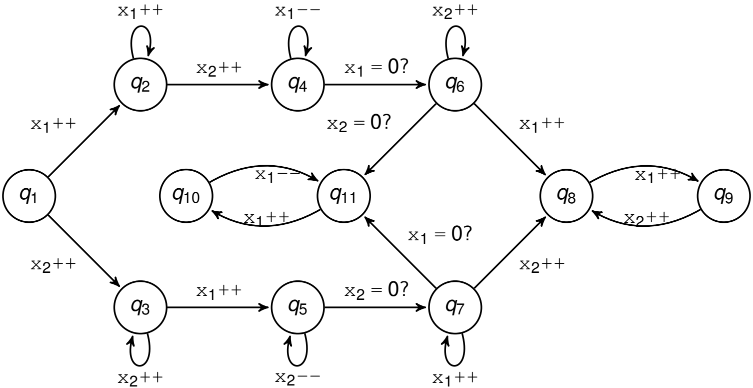
- Reversal: Alternation from nonincreasing mode to nondecreasing mode and vice-versa.



- Sequence with 3 reversals:

$$0011223334444\overline{3}33222\overline{3}334444555555\overline{4}$$

- A run is r-reversal-bounded whenever the number of reversals of each counter is less or equal to r.



$$\varphi = (x_1 \geq 2 \wedge x_2 \geq 1 \wedge (x_2 + 1 \geq x_1) \vee (x_2 \geq 2 \wedge x_1 \geq 1 \wedge x_1 + 1 \geq x_2)$$

$$[\![\varphi]\!] = \{\mathbf{y} \in \mathbb{N}^2 : \langle q_1, \mathbf{0} \rangle \xrightarrow{*} \langle q_9, \mathbf{y} \rangle\}$$

Presburger-definable reachability sets

- Let $\langle \mathcal{M}, \langle q_0, \mathbf{x}_0 \rangle \rangle$ be r-reversal-bounded for some $r \geq 0$. For each control state q, the set

$$R = \{\mathbf{y} \in \mathbb{N}^d : \exists \text{ run } \langle q_0, \mathbf{x}_0 \rangle \xrightarrow{*} \langle q, \mathbf{y} \rangle\}$$

  is effectively semilinear [Ibarra, JACM 78].

- One can compute effectively a Presburger formula φ such that $[\![\varphi]\!] = R$.

- The reachability problem with bounded number of reversals:

  Input: PCM $\mathcal{M}$, $\langle q, \mathbf{x} \rangle$, $\langle q', \mathbf{x}' \rangle$ and $r \geq 0$.

  Question: Is there a run $\langle q, \mathbf{x} \rangle \xrightarrow{*} \langle q', \mathbf{x}' \rangle$ s.t. each counter performs during the run a number of reversals bounded by r?

- The problem is decidable for a large class of counter machines.

Proof ideas

- Reachability relation of simple loops can be expressed in Presburger arithmetic.
- Runs can be normalized so that:
  - each simple loop is visited at most a doubly-exponential number of times,
  - the different simple loops are visited in a structured way.
- Parikh images of context-free languages are effectively semilinear. [Parikh, JACM 66]

The class of counter machines $\mathcal{M} = \langle Q, T, C \rangle$

- Q is a finite set of control states and $C = \{\mathrm{x}_1, \ldots, \mathrm{x}_d\}$.
- T is a finite set of transitions.
- Each transition is labelled by $\langle g, \mathbf{a} \rangle$ where $\mathbf{a} \in \mathbb{Z}^d$ (update) and g is a guard following

  $$g ::= \top \mid \bot \mid \mathrm{x} \sim k \mid g \wedge g \mid g \vee g \mid \neg g$$

  where $\mathrm{x} \in C$, $\sim \in \{\leq, \geq, =\}$ and $k \in \mathbb{N}$.
- Update functions are those for VASS.
- Guards are more general than those for Minsky machines.
- Minsky machines and VASS belong to this class.

Mode vectors
– counter values for reversals –

- From a run

$$\rho = \langle q_0, \mathbf{x}_0 \rangle \xrightarrow{t_1} \langle q_1, \mathbf{x}_1 \rangle, \ldots$$

  we define mode vectors $\mathfrak{md}_0, \mathfrak{md}_1, \ldots$ such that each $\mathfrak{md}_i \in \{\mathrm{INC}, \mathrm{DEC}\}^d$.

- By convention, $\mathfrak{md}_0$ is the unique vector in $\{\mathrm{INC}\}^d$.

- For all $j \geq 0$ and for all $i \in [1, d]$, we have
  1. $\mathfrak{md}_{j+1}(i) \stackrel{\text{def}}{=} \mathfrak{md}_j(i)$ when $\mathbf{x}_j(i) = \mathbf{x}_{j+1}(i)$.
  2. $\mathfrak{md}_{j+1}(i) \stackrel{\text{def}}{=} \mathrm{INC}$ when $\mathbf{x}_{j+1}(i) - \mathbf{x}_j(i) > 0$.
  3. $\mathfrak{md}_{j+1}(i) \stackrel{\text{def}}{=} \mathrm{DEC}$ when $\mathbf{x}_{j+1}(i) - \mathbf{x}_j(i) < 0$.

- Number of reversals:

$$Rev_i \stackrel{\text{def}}{=} \{j \in [0, |\rho| - 1] : \mathfrak{md}_j(i) \neq \mathfrak{md}_{j+1}(i)\}$$

Reversal-boundedness formally

- Run ρ is r-reversal-bounded with respect to i $\overset{\text{def}}{\Leftrightarrow}$ $\mathrm{card}(Rev_i) \leq r$.
- Run ρ is r-reversal-bounded $\overset{\text{def}}{\Leftrightarrow}$ for every $i \in [1, d]$, we have $\mathrm{card}(Rev_i) \leq r$.
- $\langle \mathcal{M}, \langle q, \mathbf{x} \rangle \rangle$ is r-reversal-bounded $\overset{\text{def}}{\Leftrightarrow}$ every run from $\langle q, \mathbf{x} \rangle$ is r-reversal-bounded.
- $\langle \mathcal{M}, \langle q, \mathbf{x} \rangle \rangle$ is reversal-bounded $\overset{\text{def}}{\Leftrightarrow}$ there is some $r \geq 0$ such that every run from $\langle q, \mathbf{x} \rangle$ is r-reversal-bounded.

Semantical restriction

- $\mathcal{M}$ is uniformly reversal-bounded $\overset{\text{def}}{\Leftrightarrow}$ there is $r \geq 0$ such that for every initial configuration, the initialized counter machine is r-reversal-bounded.
- In the sequel, reversal-bounded counter machines come with a maximal number of reversals $r \geq 0$.
- Reversal-boundedness is essentially a semantical restriction on the runs.
- Reversal-boundedness detection problem on VASS is EXPSPACE-complete (the bound r can be computed).
- Reversal-boundedness detection problem on Minsky machines is undecidable.

Structure of the forthcoming proof

- Design a notion of extended path for which no reversal occurs and satisfaction of the guards remains constant.
- Any finite r-reversal-bounded run can be generated by a small sequence of small such extended paths.
- Reachability relation generated by any extended path is definable in Presburger arithmetic.

Intervals

- $\mathcal{M} = \langle Q, T, C \rangle$ with negation-free guards.
- AG: set of atomic guards of the form $\mathtt{x} \sim k$ occurring in $\mathcal{M}$.
- $\mathcal{K} = \{0 = k_1 < k_2 < \cdots < k_K\}$ and $K = \mathrm{card}(\mathcal{K})$.
- $\mathcal{I}$: set of non-empty intervals

$$\{[k_1, k_1], [k_1 + 1, k_2 - 1], [k_2, k_2], [k_2 + 1, k_3 - 1], [k_3, k_3], \ldots,$$
$$[k_K, k_K], [k_K + 1, +\infty)\} \setminus \{\emptyset\}$$

- At most $2K$ intervals and at least $K + 1$ intervals.

Counter values symbolically

- Linear ordering on $\mathcal{I}$ (for non-empty intervals):

  $$[k_1, k_1] \;\leq\; [k_1{+}1, k_2{-}1] \leq [k_2, k_2] \leq [k_2{+}1, k_3{-}1] \leq [k_2, k_2] \leq \ldots$$

  $$\ldots \leq [k_K, k_K] \leq [k_K + 1, +\infty)\}$$

- Interval map $\mathfrak{im} : C \to \mathcal{I}$.

- Symbolic satisfaction relation $\mathfrak{im} \vdash g$:
  - $\mathfrak{im} \vdash g_1 \vee g_2 \;\overset{\text{def}}{\Leftrightarrow}\; \mathfrak{im} \vdash g_1$ or $\mathfrak{im} \vdash g_2$.
  - $\mathfrak{im} \vdash g_1 \wedge g_2 \;\overset{\text{def}}{\Leftrightarrow}\; \mathfrak{im} \vdash g_1$ and $\mathfrak{im} \vdash g_2$.
  - $\mathfrak{im} \vdash \mathrm{x} = k \;\overset{\text{def}}{\Leftrightarrow}\; \mathfrak{im}(\mathrm{x}) = [k, k]$.
  - $\mathfrak{im} \vdash \mathrm{x} \geq k \;\overset{\text{def}}{\Leftrightarrow}\; \mathfrak{im}(\mathrm{x}) \subseteq [k, +\infty)$.
  - $\mathfrak{im} \vdash \mathrm{x} \leq k \;\overset{\text{def}}{\Leftrightarrow}\; \mathfrak{im}(\mathrm{x}) \subseteq [0, k]$.

Completeness

- Interval maps and guards are built over the same set of constants.
- $\mathfrak{im} \vdash g$ can be checked in polynomial time in the sum of the respective sizes of $\mathfrak{im}$ and g.
- $\mathfrak{im} \vdash g$ iff for all $\mathfrak{f} : C \to \mathbb{N}$ and for all $\mathrm{x} \in C$, we have $\mathfrak{f}(\mathrm{x}) \in \mathfrak{im}(\mathrm{x})$ implies $\mathfrak{f} \models g$ (in Presburger arithmetic).

Guarded modes

- Guarded mode $\mathfrak{gmd}$ is a pair $\langle \mathfrak{im}, \mathfrak{md} \rangle$ where
  - $\mathfrak{im}$ is an interval map,
  - $\mathfrak{md} \in \{\mathrm{INC}, \mathrm{DEC}\}^d$.
- $t = q \xrightarrow{\langle g, \mathbf{a} \rangle} q'$ is compatible with $\mathfrak{gmd} \overset{\text{def}}{\Leftrightarrow}$
  1. $\mathfrak{im} \vdash g$,
  2. for every $i \in [1, d]$,
     - $\mathfrak{md}(i) = \mathrm{INC}$ implies $\mathbf{a}(i) \geq 0$,
     - $\mathfrak{md}(i) = \mathrm{DEC}$ implies $\mathbf{a}(i) \leq 0$.

“*Bis repetita placent*”

- Path π is a sequence of transitions

$$q_1 \xrightarrow{\langle g_1, \mathbf{a}_1 \rangle} q_1', \ldots, q_n \xrightarrow{\langle g_n, \mathbf{a}_n \rangle} q_n'$$

  so that for every $i \in [1, n]$, we have $q_i' = q_{i+1}$.

- The effect of π is the update $\mathfrak{ef}(\pi) \stackrel{\text{def}}{=} \sum_j \mathbf{a}_j \in \mathbb{Z}^d$.
- Simple loop *sl* is a non-empty path that starts and ends by the same state and that's the only repeated state.
- Number of simple loops is $\leq \mathrm{card}(T)^{\mathrm{card}(Q)}$.
- Arbitrary total linear ordering $\prec$ on simple loops.

Values

- Scale $\mathfrak{sc}(\mathcal{M})$: maximal absolute value among the updates **a** in $\mathcal{M}$.
- If size of $\mathcal{M}$ is N, then $\mathfrak{sc}(\mathcal{M}) \leq 2^N$.
- The effect $\mathfrak{ef}(sl)$ of a simple loop sl is in

$$[-\mathrm{card}(Q)\mathfrak{sc}(\mathcal{M}), \mathrm{card}(Q)\mathfrak{sc}(\mathcal{M})]^d$$

- The number of effects from simple loops is bounded by

$$(1 + 2 \times \mathrm{card}(Q)\mathfrak{sc}(\mathcal{M}))^d$$

Extended path (bis)

- Extended path **P**:

$$\pi_0 \; S_1 \; \pi_1 \; \cdots \; S_\alpha \; \pi_\alpha$$

1. the S_i's are non-empty sets of simple loops,
2. the π_i's are non-empty paths,
3. if S occurs just before [resp. after] a path π, then all the simple loops in S loops on the first [resp. last] state of π.

Some more auxiliary notions

- A sequence of transitions is compatible with the guarded mode $\mathfrak{gmd} \stackrel{\text{def}}{\Leftrightarrow}$ all its transitions are compatible with $\mathfrak{gmd}$.
- Skeleton of **P** is the path $\pi_0 \cdots \pi_\alpha$.
- $S = \{sl_1, \ldots, sl_m\}$ with $sl_1 \prec \cdots \prec sl_m$

$$e(S) \stackrel{\text{def}}{=} (sl_1)^+ \cdots (sl_m)^+$$

  (the underlying alphabet is T)
- $e(\mathbf{P}) \stackrel{\text{def}}{=} \pi_0 \cdot e(S_1) \cdots e(S_\alpha) \cdot \pi_\alpha$.
- $\mathrm{Lan}(\mathbf{P}) \stackrel{\text{def}}{=} \mathrm{Lan}(e(\mathbf{P}))$.
- Run $\rho = \langle q_0, \mathbf{x}_0 \rangle \xrightarrow{t_1} \cdots \xrightarrow{t_\ell} \langle q_\ell, \mathbf{x}_\ell \rangle$ respects **P** $\stackrel{\text{def}}{\Leftrightarrow}$ $\pi = t_1 \cdots t_\ell \in \mathrm{Lan}(\mathbf{P})$.

Global reversal phases (Intervals may change)

- Global reversal phase: finite sequence of transitions such that each transition in it is compatible with some guarded mode $\langle \mathfrak{im}, \mathfrak{md} \rangle$, for some mode $\mathfrak{md} \in \{\mathrm{INC}, \mathrm{DEC}\}^d$.

- A run respecting a global reversal phase has no reversal for all the counters.

- r-reversal-bounded run $\rho = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$.
  - ρ can be divided as a sequence of subruns $\rho = \rho_1 \cdot \rho_2 \cdots \rho_L$.
  - Each ρ_i respects a global reversal phase.
  - $L \leq (d \times r) + 1$.

Local reversal phases

- Local reversal phase: finite sequence of transitions such that each transition in it is compatible with some guarded mode $\langle \mathfrak{im}, \mathfrak{md} \rangle$.
- A run respecting a local reversal phase has no reversals and the counter values satisfy the same atomic guards.
- r-reversal-bounded run $\rho = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$.
  - ρ can be divided as a sequence $\rho = \rho_1 \cdot \rho_2 \cdots \rho_{L'}$.
  - Each ρ_i respects a local reversal phase.
  - $L' \leq ((d \times r) + 1) \times 2Kd$.

Proof idea (1/2)

- ρ can be divided in at most $(d \times r) + 1$ subruns respecting a global reversal phase.
- We show that each such subrun can be divided in at most $2Kd$ subruns respecting a local guard phase.
- Binary relation $\preceq_{\mathbf{a}}$ with $\mathbf{a} \in \mathbb{Z}^d$ on interval maps.
- $\mathfrak{im} \preceq_{\mathbf{a}} \mathfrak{im}' \overset{\text{def}}{\Leftrightarrow}$ for every $i \in [1, d]$,
  - $\mathfrak{im}(\mathrm{x}_i) \leq \mathfrak{im}'(\mathrm{x}_i)$ if $\mathbf{a}(i) \geq 0$,
  - $\mathfrak{im}'(\mathrm{x}_i) \leq \mathfrak{im}(\mathrm{x}_i)$ if $\mathbf{a}(i) \leq 0$,
  - $\mathfrak{im}'(\mathrm{x}_i) = \mathfrak{im}(\mathrm{x}_i)$ if $\mathbf{a}(i) = 0$.
- $\mathfrak{im} \prec_{\mathbf{a}} \mathfrak{im}'$: $\mathfrak{im} \preceq_{\mathbf{a}} \mathfrak{im}'$ and $\mathfrak{im} \neq \mathfrak{im}'$.

$\mathbf{x}$ agrees with $\mathfrak{im}$ and $\mathbf{x}' + \mathbf{a}$ agrees with $\mathfrak{im}'$ imply $\mathfrak{im} \preceq_{\mathbf{a}} \mathfrak{im}'$

Proof idea (2/2)

- Number of interval maps in $\mathcal{O}(K^d)$.
- Let $\mathbf{a} \in \mathbb{Z}^d$ and $\mathfrak{im}_1 \prec_{\mathbf{a}} \mathfrak{im}_2 \prec_{\mathbf{a}} \cdots \prec_{\mathbf{a}} \mathfrak{im}_\beta$. Then, $\beta \leq 2Kd$.
- In a subrun respecting a global reversal phase, each counter is compared against at most K constants and all the counters have a monotonous behaviour.
- Each counter during the global reversal phase can visit at most $2K$ distinct intervals in $\mathcal{I}$.
- Hence, the bound $2Kd$ for the maximal number of local reversal phases.

Sequences of extended paths

- $\mathbf{P}_1 \cdots \mathbf{P}_{L'}$ such that
  - each $\mathbf{P}_i$ is an extended path compatible with some guarded mode,
  - $\mathbf{P}_1 \cdots \mathbf{P}_{L'}$ is compatible with the control graph of $\mathcal{M}$.
- Any r-reversal-bounded run $\rho = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$ respects a sequence of extended paths $\mathbf{P}_1 \cdots \mathbf{P}_{L'}$ with

$$L' \leq ((d \times r) + 1) \times 2Kd$$

Small extended path (bis)

- Small extended path:
  1. π_0 and π_α have at most $2 \times \mathrm{card}(Q)$ transitions,
  2. $\pi_1, \ldots, \pi_{\alpha-1}$ have at most $\mathrm{card}(Q)$ transitions,
  3. for each $q \in Q$, there is at most one set S containing simple loops on q.
- Length of the skeleton bounded by $\mathrm{card}(Q)(3 + \mathrm{card}(Q))$.
- The set of small extended paths is finite.

Runs in normal form

- Run $\rho = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$ respecting **P** compatible with some guarded mode $\mathfrak{gmd}$.
- Then, there is small $\mathbf{P}'$ still compatible with $\mathfrak{gmd}$ and a run

  $$\rho' = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$$

  such that ρ' respects $\mathbf{P}'$.
- Generalization of the case for finite-state automata but with constraints on initial and final counter values.

Proof (1/9)

- Run $\rho = \langle q_0, \mathbf{x}_0 \rangle \xrightarrow{t_1} \cdots \xrightarrow{t_\ell} \langle q_\ell, \mathbf{x}_\ell \rangle$ respecting **P** compatible with $\mathfrak{gmd}$.
- $\pi = t_1 \cdots t_\ell \in \mathrm{Lan}(\mathbf{P})$.
- We build a small $\mathbf{P}'$ such that
  - $\mathbf{P}'$ is compatible with $\mathfrak{gmd}$,
  - there is a run ρ' respecting $\mathbf{P}'$ that starts and ends by the same configurations as ρ.

Proof (2/9)

We define a sequence of $\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_\beta$ such that

- Each $\mathbf{P}_i$ is compatible with $\mathfrak{gmd}$ and there is a run ρ_i respecting $\mathbf{P}_i$ that starts and ends by the same configurations.
- $\mathbf{P}_0$ is equal to $t_1 \cdots t_\ell$ viewed as an extended path.
- $\mathbf{P}_\beta$ is a small extended path.
- $\mathbf{P}_{i+1}$ is obtained from $\mathbf{P}_i$
  1. by removing a simple loop on q and,
  2. possibly adding it to a set of simple loops S already in $\mathbf{P}_i$ or by creating one if none exists.

Proof (3/9): from $\mathbf{P}_i$ to $\mathbf{P}_{i+1}$ (bis)

$$\mathbf{P}_i = \pi_0 \; S_1 \; \pi_1 \; \cdots \; S_\alpha \; \pi_\alpha$$

(a) $\alpha \leq \mathrm{card}(Q)$,

(b) each path in $\pi_1, \ldots, \pi_{\alpha-1}$ have length less than $\mathrm{card}(Q)$,

(c) each state has at most one S_i with simple loops on it.

$\mathbf{P}_0$ verifies these conditions.

Proof (4/9): three cases

- $\mathbf{P}_i$ is a small extended path. We are done.

- $\pi_\alpha = \pi \cdot sl \cdot \pi'$ where
  1. sl is a simple loop on q,
  2. $\pi\pi' \neq \varepsilon$,
  3. S_γ already contains simple loops on q.

  $\mathbf{P}_{i+1}$ is equal to:

  $$\pi_0 \ \cdots \ S_{\gamma-1} \ \pi_{\gamma-1} \ (S_\gamma \cup \{sl\}) \ \cdots \ \pi_{\alpha-1} \ S_\alpha \ (\pi\pi')$$

- $\pi_\alpha = \pi \cdot sl \cdot \pi'$ where
  1. sl is a simple loop on q,
  2. the first one occurring in $\pi \cdot sl$,
  3. $\pi\pi' \neq \varepsilon$,
  4. no S_γ already contains simple loops on q.

  $\mathbf{P}_{i+1}$ is equal to: $\pi_0 \ \cdots \ S_\alpha \ \pi \ \{sl\} \ \pi'$.

Proof (5/9)

- It remains to show that there is a run ρ_{i+1} respecting $\mathbf{P}_{i+1}$ that starts by $\langle q_0, \mathbf{x}_0 \rangle$ and ends by $\langle q_\ell, \mathbf{x}_\ell \rangle$.
- Satisfaction of the conditions (a)–(c) are by an easy verification.
- All the transitions in $\mathbf{P}_{i+1}$ are compatible with $\mathfrak{gmd}$ (by construction).
- The counter values have a monotonous behaviour (increase or decrease) and the atomic guards are convex.

Let us treat the case 2

- Recapitulation.
  - Run ρ_i respecting $\mathbf{P}_i$, starting by $\langle q_0, \mathbf{x}_0 \rangle$ and ending by $\langle q_\ell, \mathbf{x}_\ell \rangle$.
  - $\mathbf{P}_i = \pi_0 \ S_1 \ \pi_1 \ \cdots \ S_\alpha \ (\pi \cdot sl \cdot \pi')$.
  - $\mathbf{P}_{i+1} = \pi_0 \ \cdots \ S_{\gamma-1} \ \pi_{\gamma-1} \ (S_\gamma \cup \{sl\}) \ \cdots \ \pi_{\alpha-1} \ S_\alpha \ (\pi\pi')$.

- $S_\gamma = S_\gamma^1 \uplus S_\gamma^2$ and for all $sl' \in S_\gamma^1$ [resp. $sl' \in S_\gamma^2$], we have $sl' \prec sl$ [resp. $sl \prec sl'$].

- As $\mathbf{P}_i$ is compatible with $\mathfrak{gmd} = \langle \mathfrak{im}, \mathfrak{md} \rangle$, for $j \in [1, d]$:
  - $\mathfrak{md}(j) = \mathrm{INC}$ implies that for all $\mathbf{x} \in \mathbb{N}^d$ in ρ_i, we get that $\mathbf{x}_0(j) \leq \mathbf{x}(j) \leq \mathbf{x}_\ell(j)$.
  - $\mathfrak{md}(j) = \mathrm{DEC}$ implies that for all $\mathbf{x} \in \mathbb{N}^d$ in ρ_i, we get that $\mathbf{x}_\ell(j) \leq \mathbf{x}(j) \leq \mathbf{x}_0(j)$.

Proof (7/9)

- $\mathbf{y} \in \mathbb{N}^d$: penultimate vector of counter values in ρ.

- For all $\mathbf{x} \in \mathbb{N}^d$ occurring in ρ_i until that occurrence of $\mathbf{y}$, for every atomic guard $\mathrm{x}_j \sim k$ in AG, equivalence between
  1. $\mathfrak{im} \vdash \mathrm{x}_j \sim k$,
  2. $\mathbf{x}(j) \sim k$,
  3. $\mathbf{x}_0(j) \sim k$,
  4. $\mathbf{y}(j) \sim k$.

- Run ρ_i:

$$\rho_i = \overbrace{\pi_0 \cdots S_{\gamma-1}\ \pi_{\gamma-1}\ S_\gamma^1}^{\rho_1^\star} \cdot \overbrace{S_\gamma^2\ \pi_\gamma \cdots \pi_{\alpha-1}\ S_\alpha\ \pi}^{\rho_2^\star} \cdot \overbrace{sl}^{\rho_3^\star} \cdot \overbrace{\pi'}^{\rho_4^\star}$$

- For each $\rho_i^\star$, we write $\langle q_0^i, \mathbf{x}_0^i \rangle$ [resp. $\langle q_f^i, \mathbf{x}_f^i \rangle$] to denote its first [resp. last] configuration.

$$\rho_i = \overbrace{\pi_0 \cdots S_{\gamma-1}\ \pi_{\gamma-1}\ S^1_\gamma}^{\rho_1^\star} \cdot \overbrace{S^2_\gamma\ \pi_\gamma \cdots \pi_{\alpha-1}\ S_\alpha\ \pi}^{\rho_2^\star} \cdot \overbrace{sl}^{\rho_3^\star} \cdot \overbrace{\pi'}^{\rho_4^\star}$$

- $\rho_3^{\star\star}$: sequence of configurations obtained from $\langle q_0^2, \mathbf{x}_0^2 \rangle$ by firing the transitions of the simple loop *sl*.
- $\rho_2^{+\mathfrak{ef}(sl)}$: sequence of configurations obtained from the last configuration of $\rho_3^{\star\star}$ by firing the sequence of transitions used for $\rho_2^\star$.

$$\rho_{i+1} = \overbrace{\pi_0 \cdots S_{\gamma-1}\ \pi_{\gamma-1}\ S^1_\gamma}^{\rho_1^\star} \cdot \overbrace{sl}^{\rho_3^{\star\star}} \cdot \overbrace{S^2_\gamma\ \pi_\gamma \cdots \pi_{\alpha-1}\ S_\alpha\ \pi}^{\rho_2^{+\mathfrak{ef}(sl)}} \cdot \overbrace{\pi'}^{\rho_4^\star}$$

Properties of ρ_{i+1}

- The sequence of configurations respects the updates on the transitions.
- It remains to show that transitions in $\rho_3^{\star\star}$ and in $\rho_2^{+\mathfrak{ef}(sl)}$ can be fired by respecting the guards.
- Suppose that $\mathfrak{md}(j) = \mathrm{INC}$ for some $j \in [1, d]$ and $\mathbf{y}$ in $\rho_3^{\star\star}$:

$$\mathbf{x}_0(j) = \mathbf{x}_0^1(j) \leq \mathbf{x}_f^1(j) = \mathbf{x}_0^2(j) \leq \mathbf{y}(j) \leq \mathbf{x}_0^4(j) \leq \mathbf{x}_f^4(j) = \mathbf{x}_\ell(j)$$

- By convexity of the atomic guards $\mathrm{x}_j \sim k$ in AG, $\mathbf{y}(j) \sim k$ iff $\mathbf{y}'(j) \sim k$ where $\mathbf{y}'$ is the corresponding vector of counter values in the run $\rho_3^{\star}$ (at the same position).
- So, $\rho_3^{\star\star}$ is indeed a run of $\mathcal{M}$ respecting sl.
- Similary, $\rho_2^{+\mathfrak{ef}(sl)}$ respects $S_\gamma^2 \, \pi_\gamma \cdots \pi_{\alpha-1} \, S_\alpha \, \pi$.

Time to wrap-up!

- $\rho = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$ respecting **P** compatible with $\mathfrak{gmd}$. There exist a small **P**′ compatible with $\mathfrak{gmd}$ and $\rho' = \langle q_0, \mathbf{x}_0 \rangle \cdots \langle q_\ell, \mathbf{x}_\ell \rangle$ such that ρ' respects **P**′.

- Small sequence of extended paths:
  1. number of elements $\leq ((d \times r) + 1) \times 2Kd$,
  2. each extended path is small too.

- For any r-reversal-bounded run ρ, there is an r-reversal-bounded run ρ' between the same configurations that respects a small sequence of extended paths.

Content of the next lecture on November 6th

- Reachability sets are computable Presburger sets.
- Repeated reachability problems for reversal-bounded counter machines.
- Decidable and undecidable extensions.

Exercises

- Show that the class of ultimately period sets is closed under union and intersection.
- Show that for every linear set there is an initialized 0-reversal-bounded counter machine whose reachability set is equal to it.