Exhibition of a Structural Bug with Wings

Florent Avellaneda
joint work with Rémi Morin

Laboratoire d'Informatique Fondamentale de Marseille, AMU & CNRS, UMR 7279

27 June 2014

Outline

1. Background
2. Representation of pathological cycles
3. Searching for minimal counter-examples

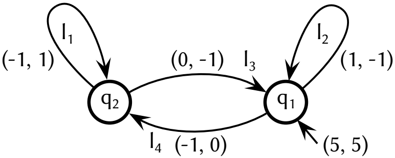
Outline

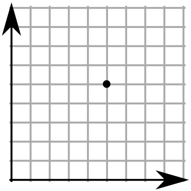
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ *with :*

- Q *a finite set of nodes,*
- $A \subseteq Q \times \mathbb{Z}^d \times Q$ *a finite set of arcs labeled by integral vectors,*
- *An initial configuration* $\mu \in Q \times \mathbb{N}^d$*.*



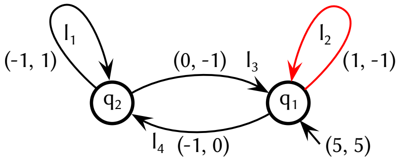


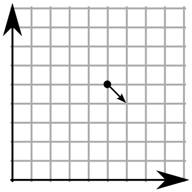
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ with :

- *Q a finite set of nodes,*
- *$A \subseteq Q \times \mathbb{Z}^d \times Q$ a finite set of arcs labeled by integral vectors,*
- *An initial configuration $\mu \in Q \times \mathbb{N}^d$.*



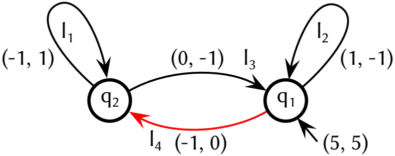


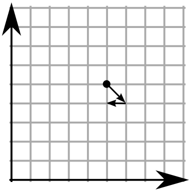
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ with :

- *Q a finite set of nodes,*
- *$A \subseteq Q \times \mathbb{Z}^d \times Q$ a finite set of arcs labeled by integral vectors,*
- *An initial configuration $\mu \in Q \times \mathbb{N}^d$.*



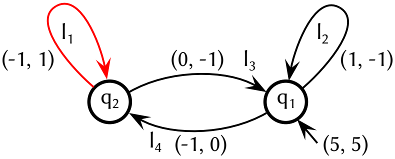


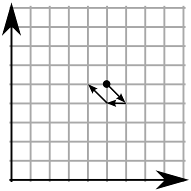
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ *with :*

- Q *a finite set of nodes,*
- $A \subseteq Q \times \mathbb{Z}^d \times Q$ *a finite set of arcs labeled by integral vectors,*
- *An initial configuration* $\mu \in Q \times \mathbb{N}^d$.



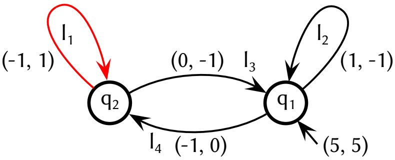


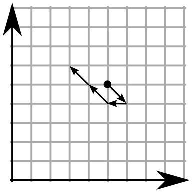
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ with :

- *Q a finite set of nodes,*
- *$A \subseteq Q \times \mathbb{Z}^d \times Q$ a finite set of arcs labeled by integral vectors,*
- *An initial configuration $\mu \in Q \times \mathbb{N}^d$.*



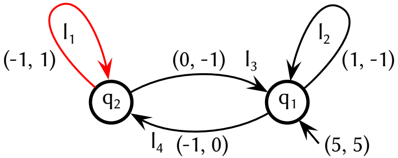


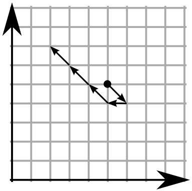
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ with :

- *Q a finite set of nodes,*
- *$A \subseteq Q \times \mathbb{Z}^d \times Q$ a finite set of arcs labeled by integral vectors,*
- *An initial configuration $\mu \in Q \times \mathbb{N}^d$.*



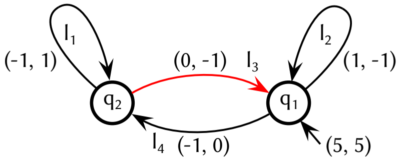


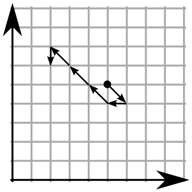
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ *with :*

- Q *a finite set of nodes,*
- $A \subseteq Q \times \mathbb{Z}^d \times Q$ *a finite set of arcs labeled by integral vectors,*
- *An initial configuration* $\mu \in Q \times \mathbb{N}^d$.



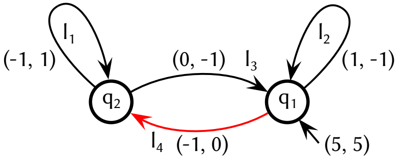


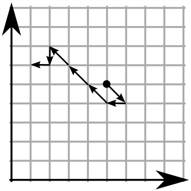
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ *with :*

- Q *a finite set of nodes,*
- $A \subseteq Q \times \mathbb{Z}^d \times Q$ *a finite set of arcs labeled by integral vectors,*
- *An initial configuration* $\mu \in Q \times \mathbb{N}^d$.



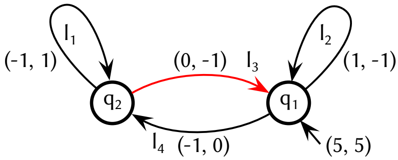


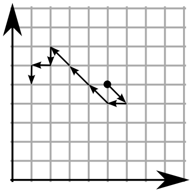
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ with :

- *Q a finite set of nodes,*
- *$A \subseteq Q \times \mathbb{Z}^d \times Q$ a finite set of arcs labeled by integral vectors,*
- *An initial configuration $\mu \in Q \times \mathbb{N}^d$.*



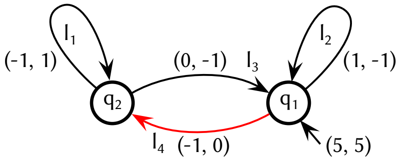


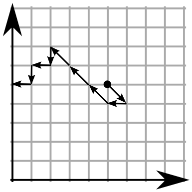
Well-known model : VASS

Definition

A vector addition system with states (VASS) is a directed graph $G = (Q, A, \mu)$ with :

- *Q a finite set of nodes,*
- *$A \subseteq Q \times \mathbb{Z}^d \times Q$ a finite set of arcs labeled by integral vectors,*
- *An initial configuration $\mu \in Q \times \mathbb{N}^d$.*





Properties

We study two structural properties :

- Structural boundedness :

  for each initial configuration, the VASS is bounded.
- Structural termination :

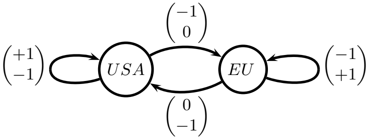
  for each initial configuration, the VASS terminates.

Motivation :

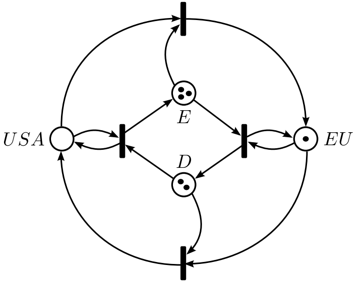
Boundedness and termination are EXPSPACE-complete problems while structural boundedness and structural termination are polynomial.

Warning

The usual simulation of a VASS by a Petri net does not preserve these properties.



(a) A VASS



(b) The "equivalent" Petri net

Characterizations

Remark

A VASS is structurally bounded if and only if there exists no cycle whose cost is $\gneq \vec{0}$.

Remark

A VASS is structurally terminating if and only if there exists no cycle whose cost is $\geq \vec{0}$.

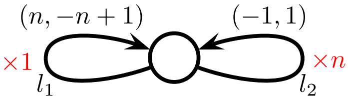
These problems are solvable in polynomial time by linear programs and computing connected components [Kosaraju and Sullivan, STOC'88].

The resulting algorithm returns in polynomial time **a multiset of arcs** H that represents a pathological cycle if such a cycle exists.

Difficulty

The user of a formal verification tool usually expects to get a simple counter example when the property is not satisfied.

Difficulty : the minimum length of a "pathological" cycle is potentially exponential.



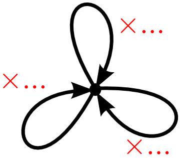
$$l_1 \underbrace{\ldots l_2 l_2 l_2 l_2 \ldots}_{n \text{ times}} \Rightarrow l_1 + n \cdot l_2$$

Aim : Concise representation of pathological cycles for VASS.

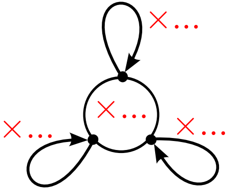
Outline

Looking for a pattern

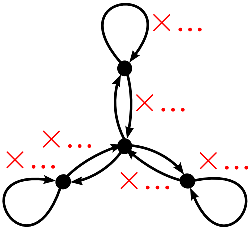
How can we decompose a pathological cycle ?



(c) Multiset of simple cycles.



(d) Flower.



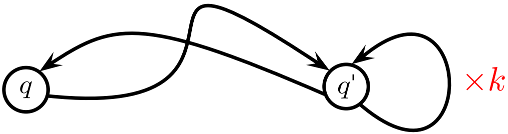
(e) Multiset of wings.

What is a wing ?

Definition

A wing with valuation k starting from a node q corresponds to a cycle made of three components :

- A path from the node q to a node q'.
- A cycle over q' iterated k times.
- A path from q' to q.



Theorem

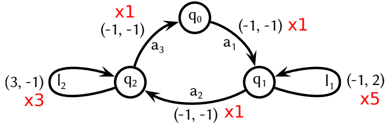
Let $H \in \mathbb{N}^A$ be a multiset of arcs corresponding to a cycle and $q_{in} \in Q_H$. We can compute in polynomial time a finite multiset of wings $\mathscr{F}$ such that :

- each wing starts from q_{in},
- $cost(\mathscr{F}) = m \cdot cost(H)$ for some $m \in \mathbb{N}^*$.

Moreover,

- Each component of each wing is simple,
- $\mathscr{F}$ contains at most d distinct wings.

$H = a_1 + 5l_1 + a_2 + 3l_2 + a_3$



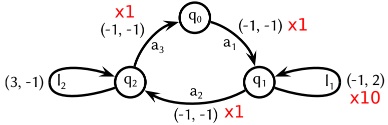
Theorem

Let $H \in \mathbb{N}^A$ be a multiset of arcs corresponding to a cycle and $q_{in} \in Q_H$. We can compute in polynomial time a finite multiset of wings $\mathscr{F}$ such that :

- each wing starts from q_{in},
- $cost(\mathscr{F}) = m \cdot cost(H)$ for some $m \in \mathbb{N}^*$.

Moreover,

- Each component of each wing is simple,
- $\mathscr{F}$ contains at most d distinct wings.



$H = a_1 + 5l_1 + a_2 + 3l_2 + a_3$

$W_1 = a_1 + 10l_1 + a_2 + a_3$

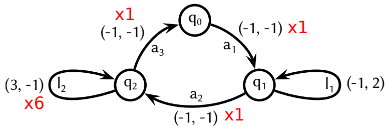
Theorem

Let $H \in \mathbb{N}^A$ be a multiset of arcs corresponding to a cycle and $q_{in} \in Q_H$. We can compute in polynomial time a finite multiset of wings $\mathscr{F}$ such that :

- each wing starts from q_{in},
- $cost(\mathscr{F}) = m \cdot cost(H)$ for some $m \in \mathbb{N}^*$.

Moreover,

- Each component of each wing is simple,
- $\mathscr{F}$ contains at most d distinct wings.



$$H = a_1 + 5l_1 + a_2 + 3l_2 + a_3$$
$$W_1 = a_1 + 10l_1 + a_2 + a_3$$
$$W_2 = a_1 + a_2 + 6l_2 + a_3$$

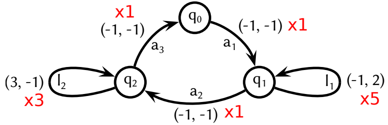
Theorem

Let $H \in \mathbb{N}^A$ be a multiset of arcs corresponding to a cycle and $q_{in} \in Q_H$. We can compute in polynomial time a finite multiset of wings $\mathscr{F}$ such that :

- each wing starts from q_{in},
- $cost(\mathscr{F}) = m \cdot cost(H)$ for some $m \in \mathbb{N}^*$.

Moreover,

- Each component of each wing is simple,
- $\mathscr{F}$ contains at most d distinct wings.



$$H = a_1 + 5l_1 + a_2 + 3l_2 + a_3$$
$$W_1 = a_1 + 10l_1 + a_2 + a_3$$
$$W_2 = a_1 + a_2 + 6l_2 + a_3$$
$$\mathscr{F} = W_1 + W_2$$
$$cost(\mathscr{F}) = 2 \cdot cost(H)$$

Idea of the proof

Definition

Let $H \in \mathbb{N}^A$ be a non-empty multiset of arcs and $q_{in} \in Q_H$.
Let C be a simple cycle within H and $k = max_{a \in C} H(a)$. Then C is **adequate** for H and q_{in} if it satisfies the two next conditions :

- the multiset of arcs $H - k \cdot C$ is connected ;
- if $H - k \cdot C$ is not empty then $Q_{H-k \cdot C}$ contains q_{in}.

Key lemma

For each H, we can compute in polynomial time an adequate cycle in H.

Illustration of the proof

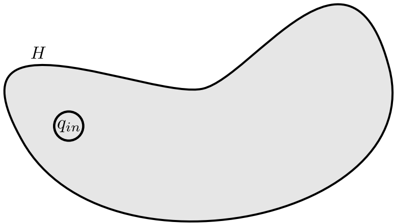


Illustration of the proof

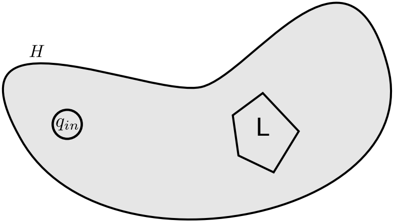


Illustration of the proof

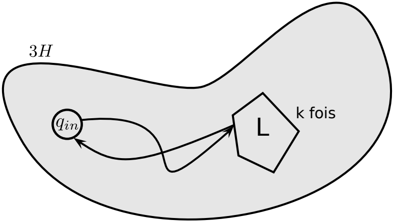
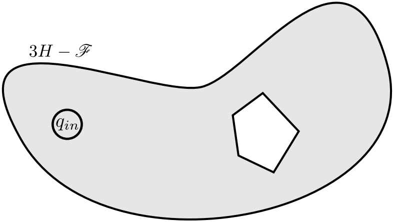
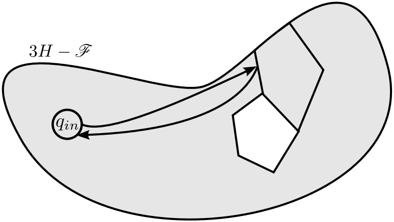


Illustration of the proof



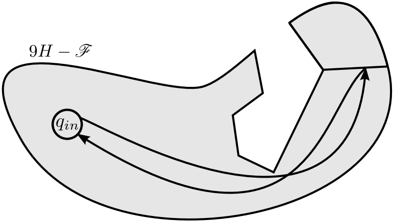
$\mathscr{F} = k_1 \cdot W_1$

Illustration of the proof



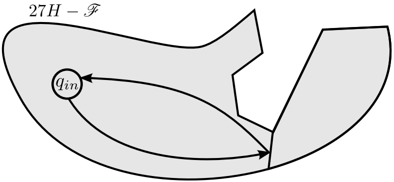
$\mathscr{F} = k_1 \cdot W_1$

Illustration of the proof



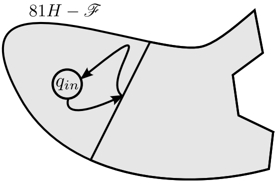
$\mathscr{F} = 3 \cdot k_1 \cdot W_1 + k_2 \cdot W_2$

Illustration of the proof



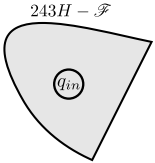
$$\mathscr{F} = 9 \cdot k_1 \cdot W_1 + 3 \cdot k_2 \cdot W_2 + k_3 \cdot W_3$$

Illustration of the proof



$$\mathscr{F} = 27 \cdot k_1 \cdot W_1 + 9 \cdot k_2 \cdot W_2 + 3 \cdot k_3 \cdot W_3 + k_4 \cdot W_4$$

Illustration of the proof



$$\mathscr{F} = 81 \cdot k_1 \cdot W_1 + 27 \cdot k_2 \cdot W_2 + 9 \cdot k_3 \cdot W_3 + 3 \cdot k_4 \cdot W_4 + k_5 \cdot W_5$$

Illustration of the proof

$$\mathscr{F} = 243 \cdot k_1 \cdot W_1 + 81 \cdot k_2 \cdot W_2 + 27 \cdot k_3 \cdot W_3 + 9 \cdot k_4 \cdot W_4 + 3 \cdot k_5 \cdot W_5 + k_6 \cdot W_6$$

Illustration of the proof

$$\mathscr{F} = 243 \cdot k_1 \cdot W_1 + 81 \cdot k_2 \cdot W_2 + 27 \cdot k_3 \cdot W_3 + 9 \cdot k_4 \cdot W_4 + 3 \cdot k_5 \cdot W_5 + k_6 \cdot W_6$$

By Carathéodory's theorem, we can reduce $\mathscr{F}$ to d wings.

Outline

Context

The following problems are NP-hard :

- Minimizing the length of pathological cycles.
- Minimizing the number of distinct arcs in pathological cycles.
- Minimizing the number of dimensions in pathological cycles.
- Minimizing the maximum number of times each arc is used.

However,

Second result

Minimizing the length of wings can be done in polynomial time.

An Upper Bound for the Valuation of Wings

Lemma

Let $\mathscr{F}$ be a multiset of wings starting from q with length at most l such that $cost(\mathscr{F}) \geq \vec{0}$. Let $\phi = 96 \times p^4 \times size(S)$. Then there exists a non-empty finite multiset $\mathscr{F}'$ of wings starting from q with length at most l and valuation at most 2^{ϕ} such that $cost(\mathscr{F}') \geq \vec{0}$.

Hint : Write an integer linear program whose variables correspond to the valuation of wings.

Remarks : We can restrict the search to wings with length at most l and valuation at most 2^{ϕ}. The number of these wings is finite.

Let $W_1, ..., W_N$ be an enumeration of these wings.

We consider the linear program for a vector $x \in \mathbb{Q}^N$ with N unknown :

$$\Sigma_{i=1}^{N} x[i] \cdot cost(W_i) \geq \vec{0} \text{ with } x \in \mathbb{Q}^N$$
$$x \gneq \vec{0}$$

Remark : The number of unknown is exponential.

=> We consider the dual problem.

Let $W_1, ..., W_N$ be an enumeration of wings starting from q with length at most l and valuation at most 2^ϕ.

We consider the linear program for a vector $y \in \mathbb{Q}^p$ with p unknown :

$$y[i] > 0, \text{ for } i \in [1..p]$$
$$-cost(W_i)^\top y > 0, \text{ for } i \in [1..N]$$

By Gordan Theorem, the linear program has no solution if and only if there exists some non-negative non-zero linear combination of its row vectors that sums to a non-negative vector.

Remarks :

- The number of unknown is linear.
- The number of inequalities is exponential.

We use the ellipsoid method [Grötschel, Lovász, Schrijver'81].

Theorem [Grötschel, Lovász, Schrijver'81]

We can solve a linear program with arbitrary number of constraints in polynomial time if we have a polynomial separation algorithm.

Idea of the separation algorithm :

- If $y \not> \vec{0}$, return some $i \in [1..p]$ such that $y[i] \leq 0$.
- For all $q, q' \in Q$, we calculate the maximal weight of the paths from q to q' with length at most l.
  $\Rightarrow$ We calculate the wing with the maximum weight.

$$y[i] > 0, \text{ for } i \in [1..p]$$
$$-cost(W_i)^\top y > 0, \text{ for } i \in [1..N]$$

- We are interested in structural properties of VASS because they are useful in practice.
- We can detect and represent a structural bug by a multiset of d wings in polynomial time.
- We can minimizing the length of these wings in polynomial time.

Thanks.