The Tractability Border of Reachability in Simple Vector Addition Systems with States

Henry Sinclair-Banks

Based on work with Dmitry Chistikov, Wojciech Czerwiński, Filip Mazowiecki, Łukasz Orlikowski, and Karol Węgrzycki in FOCS'24.

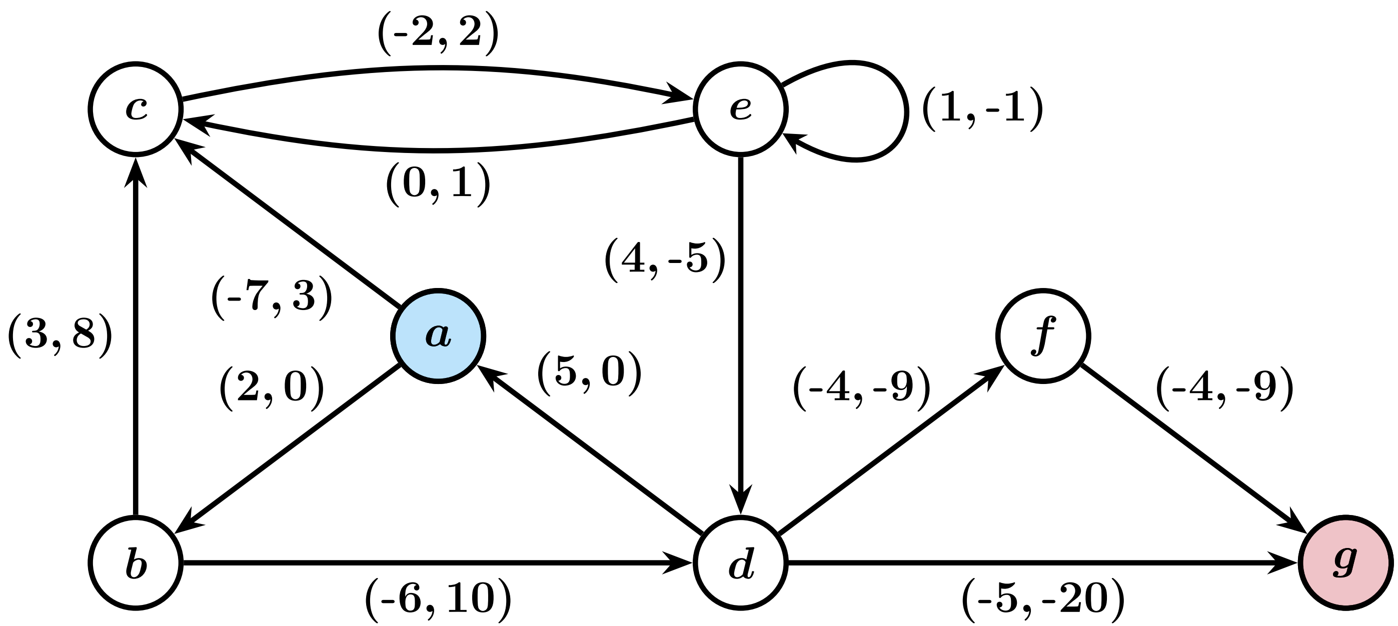
     

Verification Seminar

13th February 2025

University of Liverpool, UK

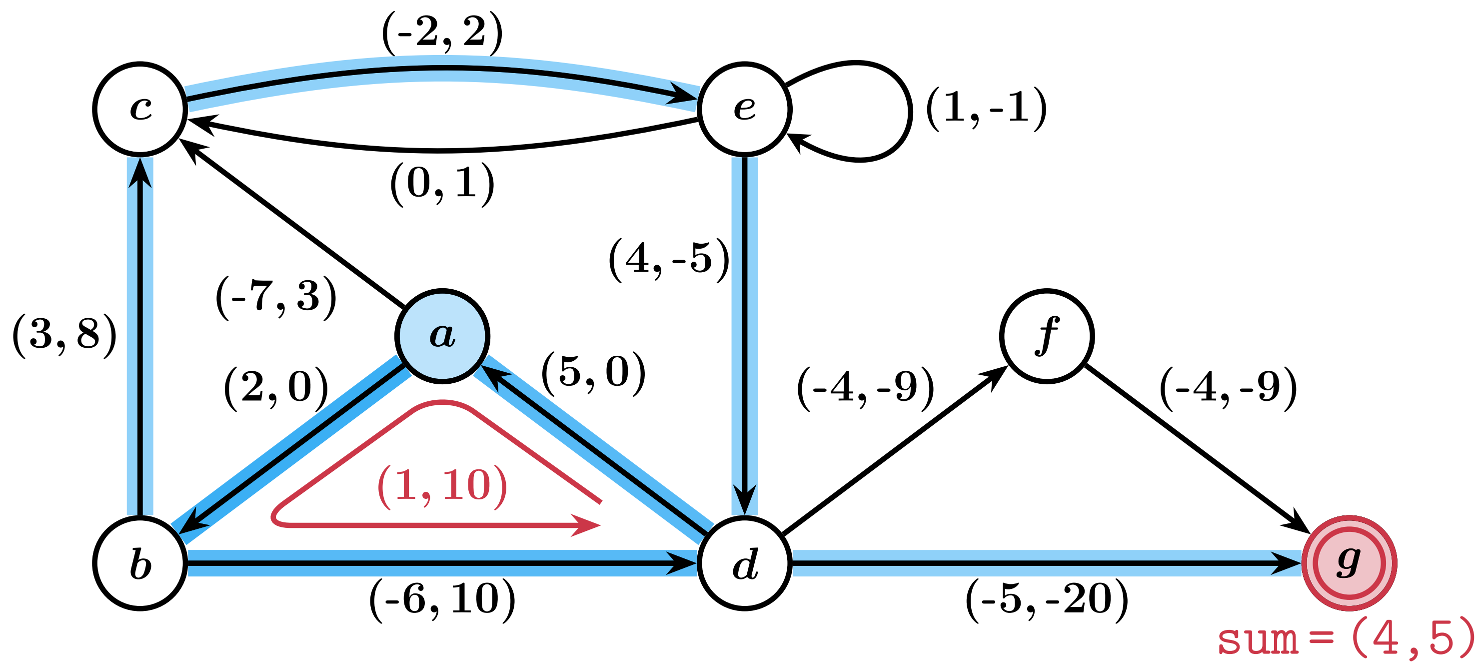
Reachability in 2-Dimensional VASS



Does there exist a run from a with counter values (0,0) to g with counter values (4,5) ?

(the counters must remain nonnegative at all times)

Reachability in 2-Dimensional VASS

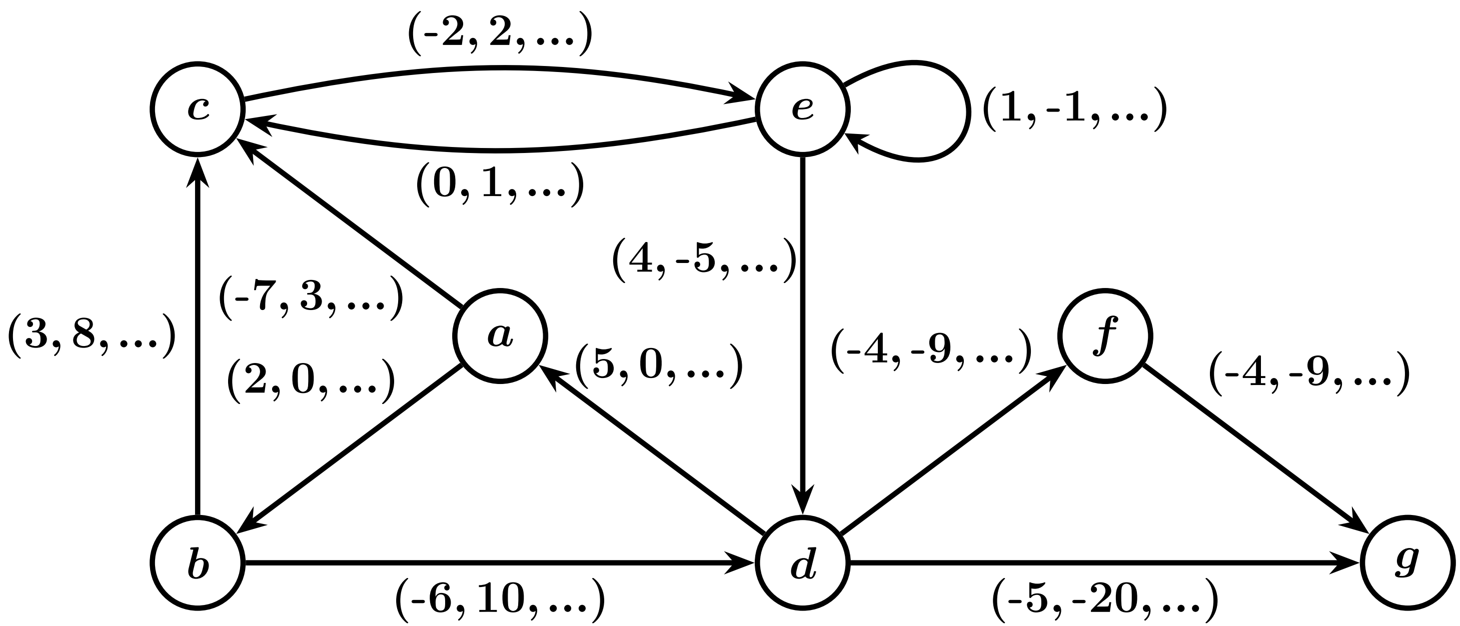


Does there exist a run from *a* with counter values (0,0) to *g* with counter values (4,5) ?

(the counters must remain nonnegative at all times)

YES!

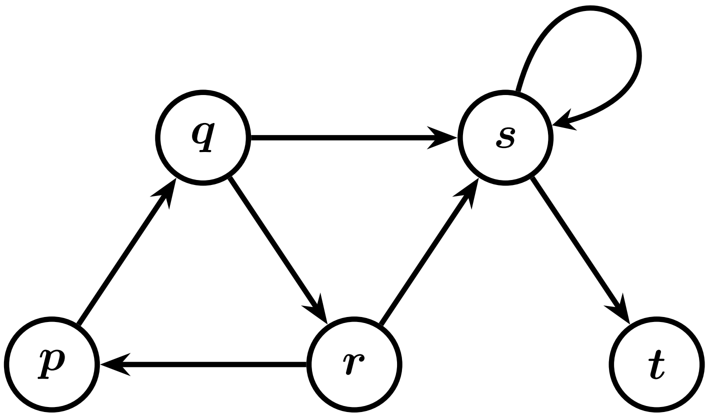
Reachability in VASS



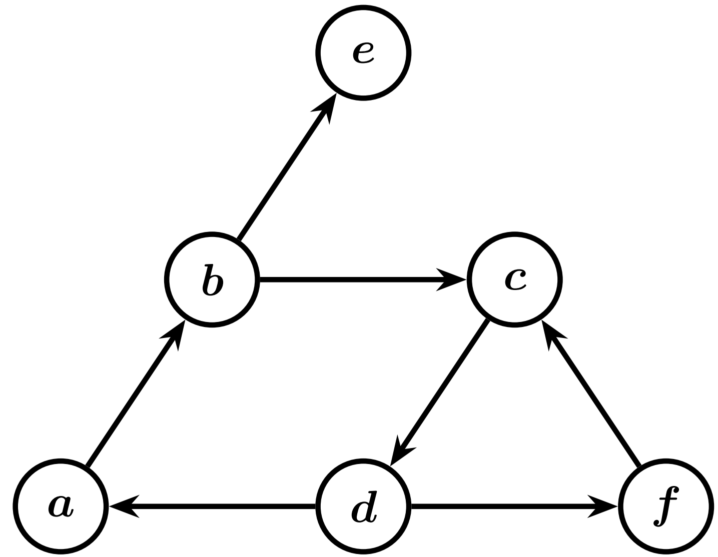
Reachability problem: does there exist a run from $p(\mathbf{u})$ to $q(\mathbf{v})$?

"Simple" Vector Addition Systems with States

Definition (Flat)**.** For every state q, there is at most one simple cycle that contains q.



Flat :)



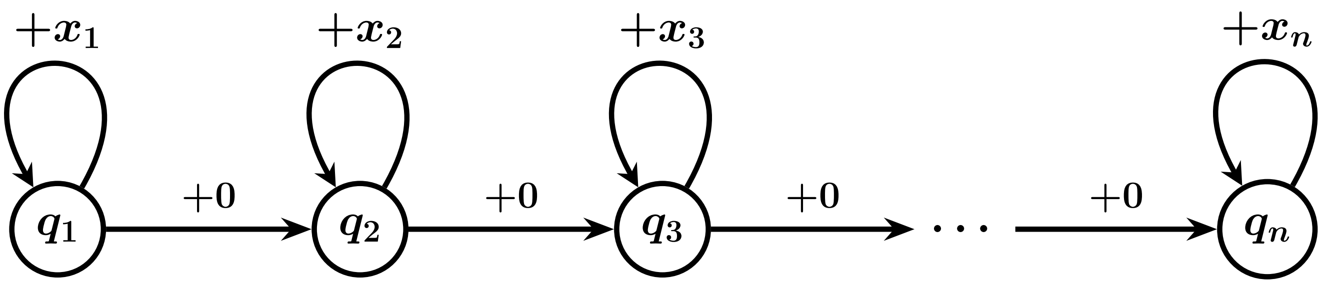
Not flat :(

Reachability in Flat VASS

Theorem. Reachability in flat VASS is in NP (even with binary encoding). [Fribourg and Olsén '97]
[Czerwiński, Lasota, Lazić, Leroux, and Mazowiecki '20]

Theorem. Reachability in binary flat 1-VASS is NP-hard. [Rosier and Yen '85]

Proof sketch. Let $(\{x_1, \ldots, x_n\}, t)$ be an instance of subset sum (with multiplicities).



There exist $k_1, \ldots, k_n$ such that $\Sigma k_i \cdot x_i = t \implies$ there is a run from $q_1(0)$ to $q_n(t)$.

There is a run from $q_1(0)$ to $q_n(t) \implies$ there exist $k_1, \ldots, k_n$ such that $\Sigma k_i \cdot x_i = t$. □

Reachability in Flat VASS

Theorem. Reachability in flat VASS is in NP (even with binary encoding). [Fribourg and Olsén '97]
[Czerwiński, Lasota, Lazić, Leroux, and Mazowiecki '20]

Theorem. Reachability in binary flat 1-VASS is NP-hard. [Rosier and Yen '85]

Theorem. Reachability in unary (flat) 1-VASS and 2-VASS is in NL. [Valiant and Paterson '73]
[Englert, Lazić, and Totzke '16]

Theorem. Reachability in unary flat d-VASS is NP-hard for $d = 7$.
[Czerwiński, Lasota, Lazić, Leroux, and Mazowiecki '20]

... for $d = 5$. [Dubiak '20]

... for $d = 4$. [Czerwiński and Orlikowski '22]

Reachability in Flat VASS

Theorem. Reachability in flat VASS is in NP (even with binary encoding). [Fribourg and Olsén '97]
[Czerwiński, Lasota, Lazić, Leroux, and Mazowiecki '20]

Theorem. Reachability in binary flat 1-VASS is NP-hard. [Rosier and Yen '85]

What is the complexity of reachability in unary flat $\mathbf{3}$-VASS?

[Blondin, Finkel, Göller, Haase, and McKenzie '15]
[Englert, Lazić, and Totzke '16]

Theorem. Reachability in unary (flat) 1-VASS and 2-VASS is in NL.

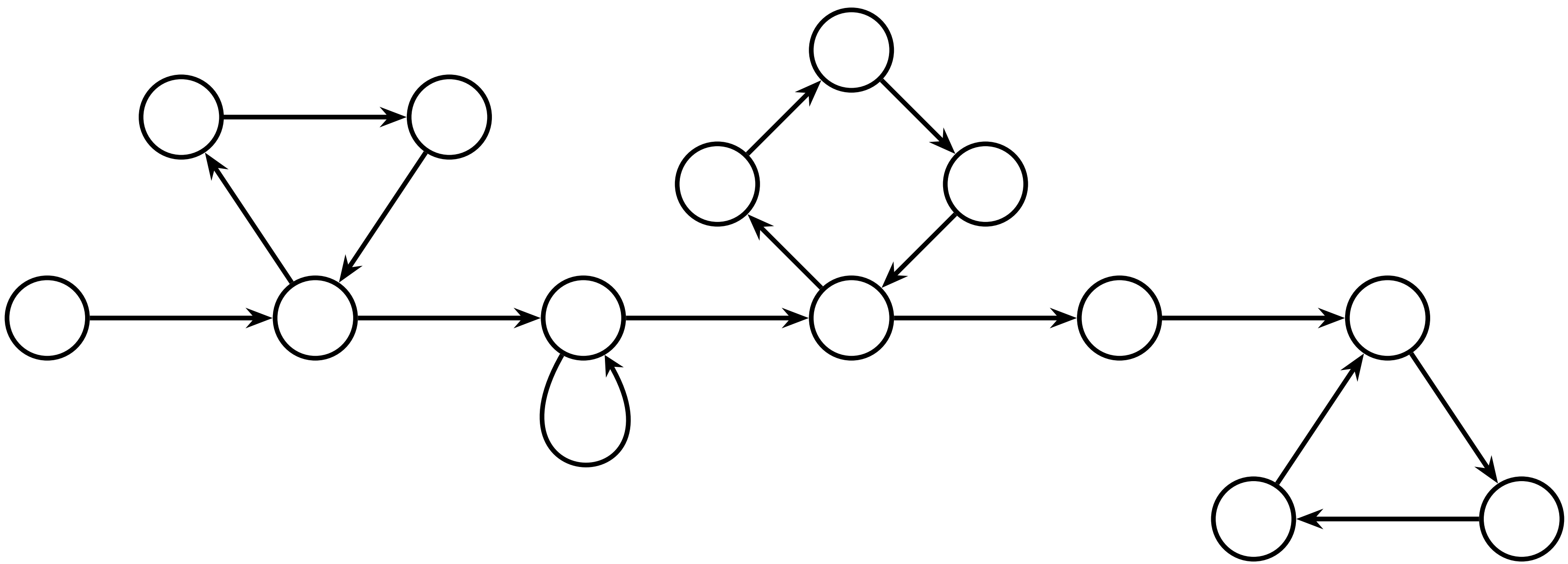
Theorem. Reachability in unary flat d-VASS is NP-hard for $d = 7$.
[Czerwiński, Lasota, Lazić, Leroux, and Mazowiecki '20]

... for $d = 5$. [Dubiak '20]

... for $d = 4$. [Czerwiński and Orlikowski '22]

~~Flat VASS~~ Linear Path Schemes

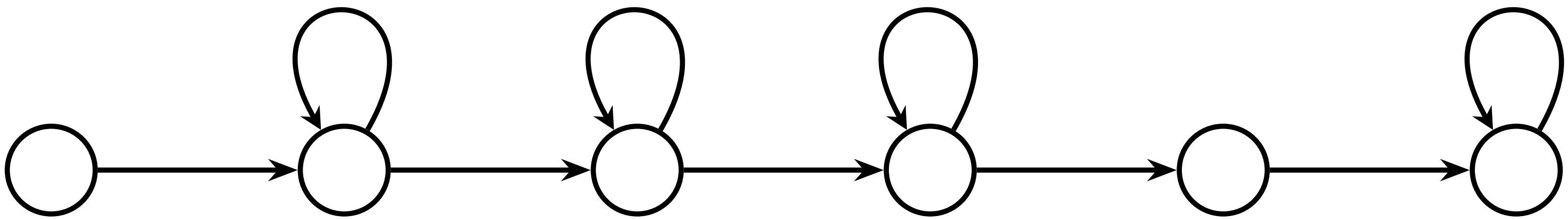
Definition (LPS)**.** A VASS where the states and transitions form a simple path between disjoint cycles.



~~Flat VASS~~ Linear Path Schemes

Definition (LPS)**.** A VASS where the states and transitions form a simple path between disjoint cycles.

Definition (SLPS)**.** A *Simple* LPS has cycles of length one ("self-loops").



For $d \geq 3$, is reachability in unary d-dimensional linear path schemes in P?

[Englert, Lazić, and Totzke '16]

[Leroux '21]

Main Contribution

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Proof approach. Recall that reachability in (binary encoded) flat VASS is in NP.

For NP-hardness, reduce from 3-SAT.

1) Use "Chinese remainder encoding" for SAT.
2) Encode satisfiability as a conjunction of non-divisibility assertions.

Next slide

3) Design a 2-SLPS with zero tests for asserting non-divisibility.
4) Concatenate these 2-SLPSs with zero tests so that reachability coincides with the conjunction of non-divisibility assertions.
5) Use an additional third counter to simulate the zero tests.

Encoding SAT as a Conjunction of Non-Divisibility Assertions

Chinese remainder encoding for SAT with k variables $x_1, \ldots, x_k$.

- Let $p_1, \ldots, p_k$ be the first k primes.
- Let $n \in \mathbb{N}$ such that $n \equiv 0 \bmod p_i \iff x_i$ is false and $n \equiv 1 \bmod p_i \iff x_i$ is true.

First, enforce assignment validity.

- Want to verify that $n \equiv 0 \bmod p_i$ OR $n \equiv 1 \bmod p_i$ (for every i).
- Instead, check $p_i \nmid n - 2$ AND $p_i \nmid n - 3$ AND $\cdots$ AND $p_i \nmid n - (p_i - 1)$.

Second, enforce satisfiability.

- A clause $x_1 \vee \neg x_2 \vee x_3$ is satisfied if $n \equiv 1 \bmod 2$ OR $n \equiv 0 \bmod 3$ OR $n \equiv 1 \bmod 5$.
- This is only falsified when $n \equiv 10 \bmod 2 \cdot 3 \cdot 5$.
- Therefore, check $2 \cdot 3 \cdot 5 \nmid n - 10$.

Encoding SAT as a Conjunction of Non-Divisibility Assertions

Chinese remainder encoding for SAT with k variables $x_1, \ldots, x_k$.

- Let $p_1, \ldots, p_k$ be the first k primes.
- Let $n \in \mathbb{N}$ such that $n \equiv 0 \bmod p_i \iff x_i$ is false and $n \equiv 1 \bmod p_i \iff x_i$ is true.

First, enforce assignment validity.

- Want to verify that $n \equiv 0 \bmod p_i$ OR $n \equiv 1 \bmod p_i$ (for every i).
- Instead, check $p_i \nmid n - 2$ AND $p_i \nmid n - 3$ AND $\cdots$ AND $p_i \nmid n - (p_i - 1)$.

Second, enforce satisfiability.

- A clause $x_1 \vee \neg x_2 \vee x_3$ is satisfied if $n \equiv 1 \bmod 2$ OR $n \equiv 0 \bmod 3$ OR $n \equiv 1 \bmod 5$.
- This is only falsified when $n \equiv 10 \bmod 2 \cdot 3 \cdot 5$.
- Therefore, check $2 \cdot 3 \cdot 5 \nmid n - 10$.

Main Contribution

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Proof approach. Recall that reachability in (binary encoded) flat VASS is in NP.

For NP-hardness, reduce from 3-SAT.

✓ 1) Use "Chinese remainder encoding" for SAT.

✓ 2) Encode satisfiability as a conjunction of non-divisibility assertions.

3) Design a 2-SLPS with zero tests for asserting non-divisibility. **Next slide**

4) Concatenate these 2-SLPSs with zero tests so that reachability coincides with the conjunction of non-divisibility assertions.

5) Use an additional third counter to simulate the zero tests.

Simple Linear Path Schemes Asserting Non-Divisibility

Suppose we want to assert $7 \nmid v$.

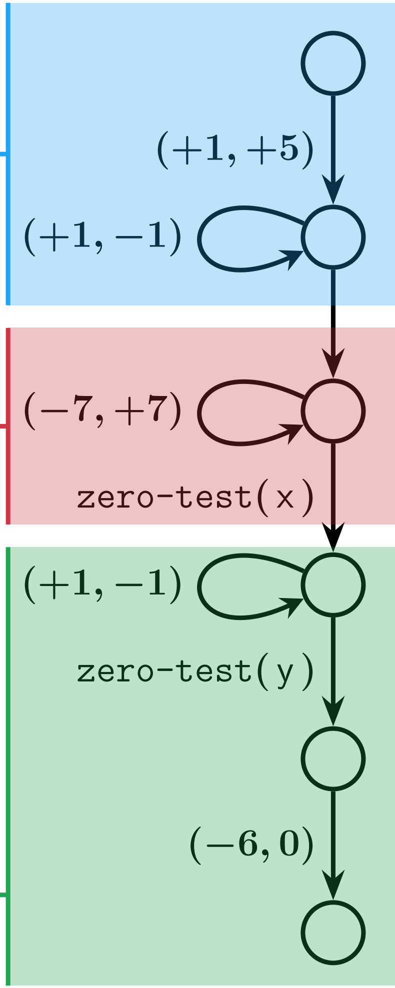
Let's construct a 2-SLPS with zero tests that:

- starts with x $= v$, y $= 0$,
- can only be passed if $7 \nmid v$, and
- ends with x $= v$, y $= 0$.

(i) Choose $r \in \{1, 2, 3, 4, 5, 6\}$ ...

(ii) ... such that $7 \mid v + r$.

(iii) Restore x $= v$, y $= 0$.



Main Contribution

Theorem. Reachability in unary 3-SLPS is NP-complete.

Proof approach. Recall that reachability in (binary encoded) flat VASS is in NP.

For NP-hardness, reduce from 3-SAT.

✓ 1) Use "Chinese remainder encoding" for SAT.

✓ 2) Encode satisfiability as a conjunction of non-divisibility assertions.

✓ 3) Design a 2-SLPS with zero tests for asserting non-divisibility.

4) Concatenate these 2-SLPSs with zero tests so that reachability coincides with the conjunction of non-divisibility assertions. And add an $\mathsf{x} + 1$ loop for guessing an assignment $\mathsf{x} = \boldsymbol{v}$.

5) Use an additional third counter to simulate the zero tests.

Main Contribution

Theorem. Reachability in unary 3-SLPS is NP-complete.

Proof approach. Recall that reachability in (binary encoded) flat VASS is in NP.

For NP-hardness, reduce from 3-SAT.

✓ 1) Use "Chinese remainder encoding" for SAT.

✓ 2) Encode satisfiability as a conjunction of non-divisibility assertions.

✓ 3) Design a 2-SLPS with zero tests for asserting non-divisibility.

✓ 4) Concatenate these 2-SLPSs with zero tests so that reachability coincides with the conjunction of non-divisibility assertions. And add an $\mathsf{x} + \mathbf{1}$ loop for guessing an assignment $\mathsf{x} = \boldsymbol{v}$.

5) Use an additional third counter to simulate the zero tests. **Next slide**

Simulating Zero Tests

Lemma 2.2 (Controlling Counter Technique). *Let $\mathcal{Z}$ be a d-VASS with zero tests and let $s(\mathbf{x}), t(\mathbf{y})$ be two configurations. Suppose $\mathcal{Z}$ has the property that on any accepting run from $s(\mathbf{x})$ to $t(\mathbf{y})$, at most m zero tests are performed on each counter. Then there exists a $(d+1)$-VASS $\mathcal{V}$ and two configurations $s'(\mathbf{0}), t'(\mathbf{y}')$ such that:*

(1) $s(\mathbf{x}) \xrightarrow{*}_{\mathcal{Z}} t(\mathbf{y})$ *if and only if* $s'(\mathbf{0}) \xrightarrow{*}_{\mathcal{V}} t'(\mathbf{y}')$,

(2) $\mathcal{V}$ *can be constructed in* $\mathcal{O}((\mathit{size}(\mathcal{Z}) + \|x\|) \cdot (m+1)^d)$ *time, and*

(3) $\|\mathbf{y}'\| \leq \|\mathbf{y}\|$.

Moreover, if $\mathcal{Z}$ is a flat VASS or a (simple) linear path scheme in which no zero-testing transition lies on a cycle, then $\mathcal{V}$ can be assumed to be a flat VASS or a (simple) linear path scheme, respectively.

First developed in [Czerwiński, Lasota, Lazić, Leroux, and Mazowiecki '19]

First formalised in [Czerwiński and Orlikowski '21]

Reformulated in [this paper]

Takeway message: A “small” number of zero tests can be simulated by an additional counter.

Main Contribution

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Proof approach. Recall that reachability in (binary encoded) flat VASS is in NP.

For NP-hardness, reduce from 3-SAT.

✓ 1) Use "Chinese remainder encoding" for SAT.

✓ 2) Encode satisfiability as a conjunction of non-divisibility assertions.

✓ 3) Design a 2-SLPS with zero tests for asserting non-divisibility.

✓ 4) Concatenate these 2-SLPSs with zero tests so that reachability coincides with the conjunction of non-divisibility assertions. And add an $\mathsf{x} + \mathbf{1}$ loop for guessing an assignment $\mathsf{x} = \boldsymbol{v}$.

✓ 5) Use an additional third counter to simulate the zero tests.

Main Results

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Theorem 2. Reachability in unary *ultraflat* 4-VASS is NP-complete.

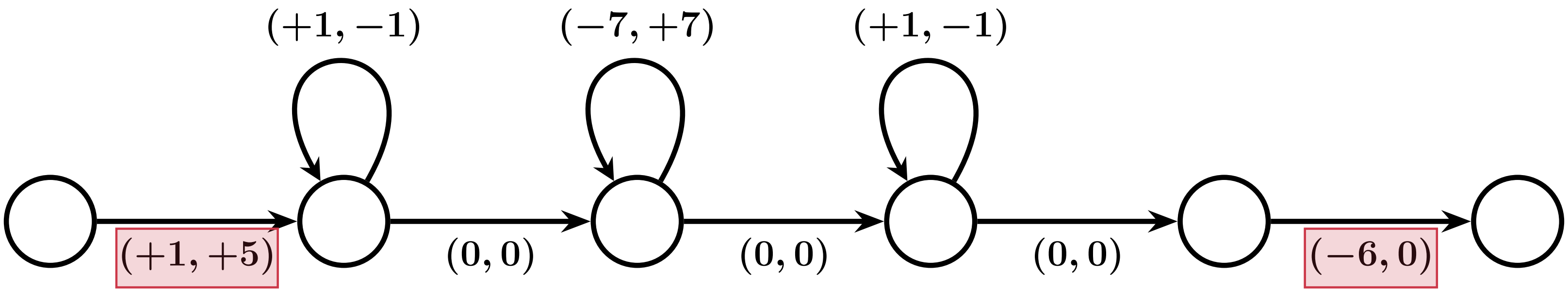
Theorem 3. Reachability in *unitary* inverse-Ackermann-dimensional SLPS is NP-complete.

Next slides

Theorem 4. Reachability in unary 2-SLPS with *binary encoded initial and target configurations* is in P.

~~Flat VASS~~ ~~Linear Path Schemes~~ Ultraflat VASS

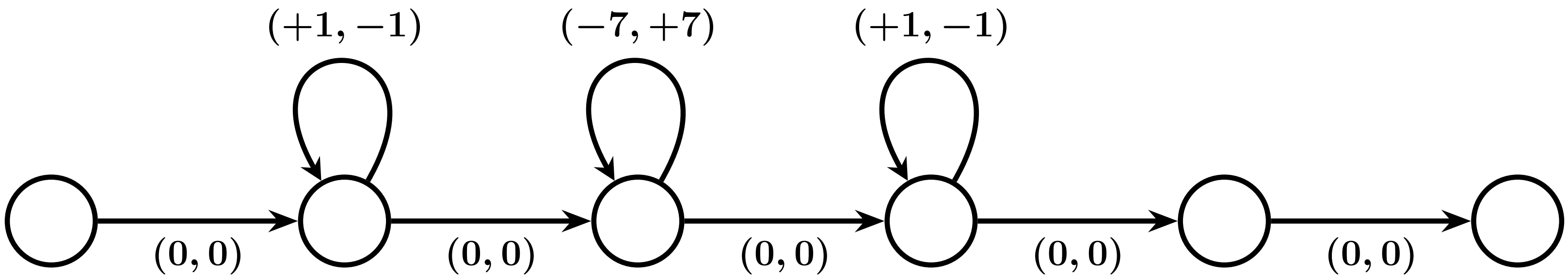
Definition (Ultraflat VASS)**.** An SLPS where the transitions between states have zero effect.



Not ultraflat :(

~~Flat VASS~~ ~~Linear Path Schemes~~ Ultraflat VASS

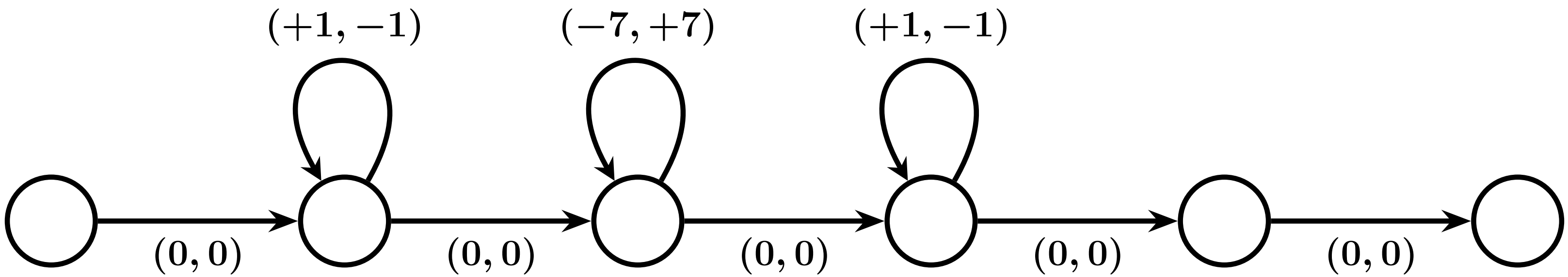
Definition (Ultraflat VASS)**.** An SLPS where the transitions between states have zero effect.



Ultraflat :)

~~Flat VASS~~ ~~Linear Path Schemes~~ Ultraflat VASS

Definition (Ultraflat VASS)**.** An SLPS where the transitions between states have zero effect.



Ultraflat :)

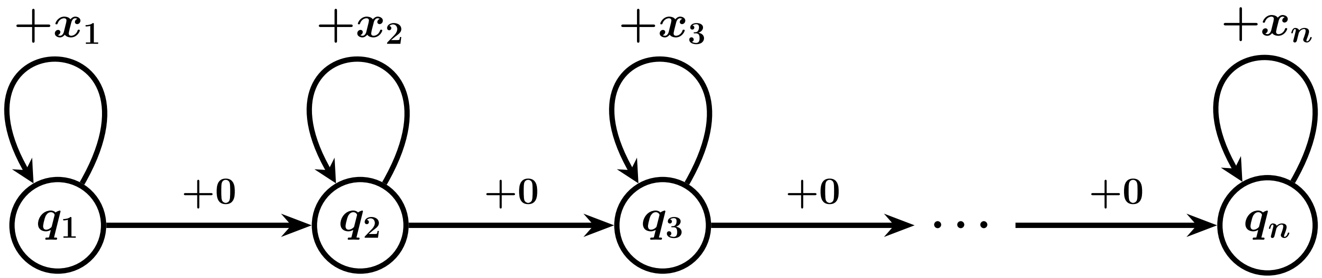
Counter program notation:

1. `LOOP:` $x \mathrel{+}= 1$, $y \mathrel{-}= 1$
2. `LOOP:` $x \mathrel{-}= 7$, $y \mathrel{+}= 7$
3. `LOOP:` $x \mathrel{+}= 1$, $y \mathrel{-}= 1$

Reachability in Ultraflat VASS

Theorem. Reachability in binary ultraflat 1-VASS is NP-hard. [Rosier and Yen '85] [Leroux '21]

Proof idea.



1. `LOOP:` z $+= x_1$
2. `LOOP:` z $+= x_2$
3. `LOOP:` z $+= x_3$
4. $\ldots$

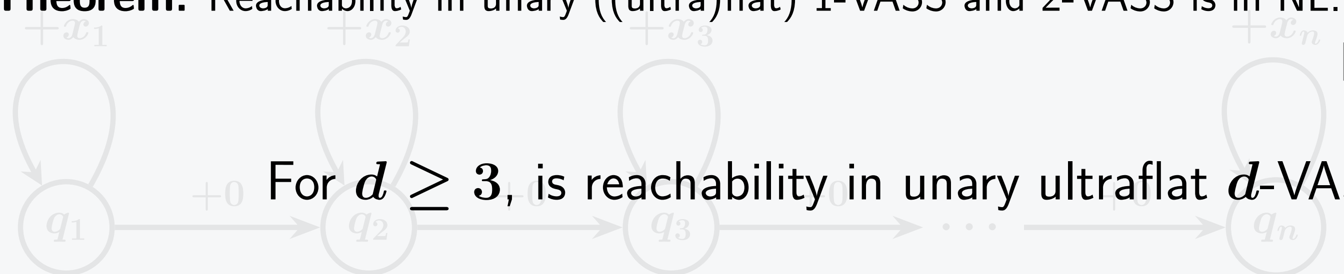
n. `LOOP:` z $+= x_n$

Reachability in Ultraflat VASS

Theorem. Reachability in binary ultraflat 1-VASS is NP-hard. [Rosier and Yen '85] [Leroux '21]

Proof idea.

Theorem. Reachability in unary ((ultra)flat) 1-VASS and 2-VASS is in NL. [Valiant and Paterson '73] [Englert, Lazić, and Totzke '16]



For $d \geq 3$, is reachability in unary ultraflat d-VASS in P? [Leroux '21]

Theorem 2. Reachability in unary ultraflat 4-VASS is NP-complete.

Proof ingredients.

3-SAT reduction.

Chinese remainder encoding for SAT.

Conjunction of non-divisibility assertions.

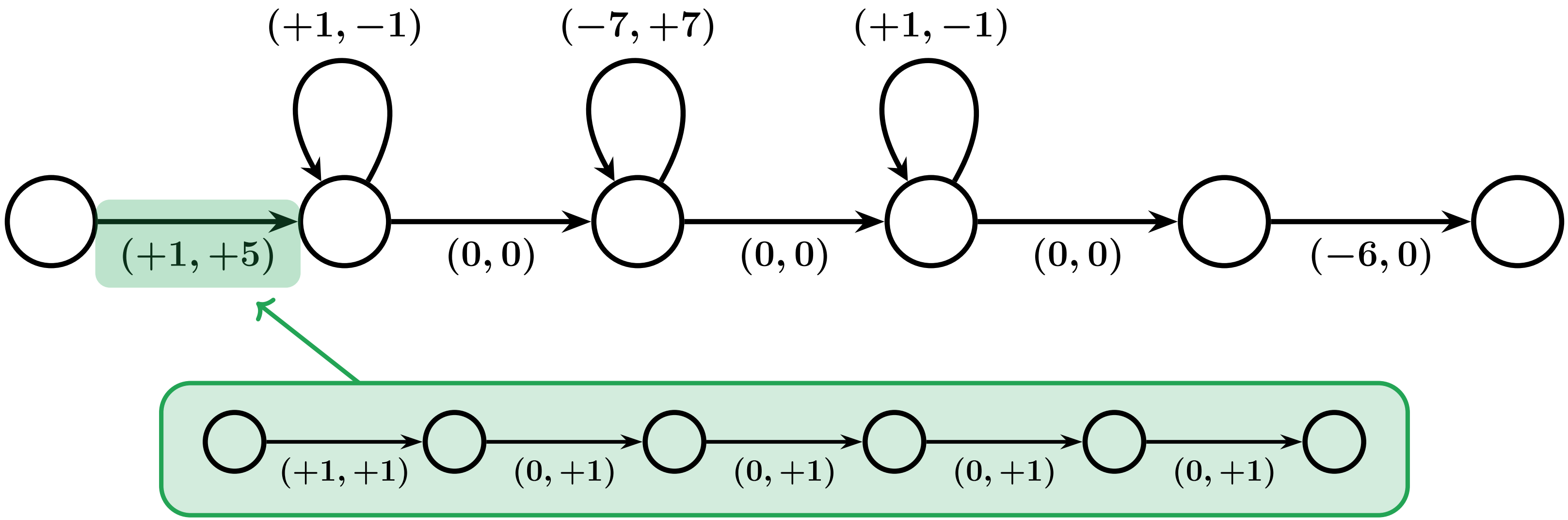
Ultraflat 3-VASS with zero tests for asserting non-divisibility.

Concatenate non-divisibility asserting ultraflat VASS.

Simulate zero tests with a controlling counter.

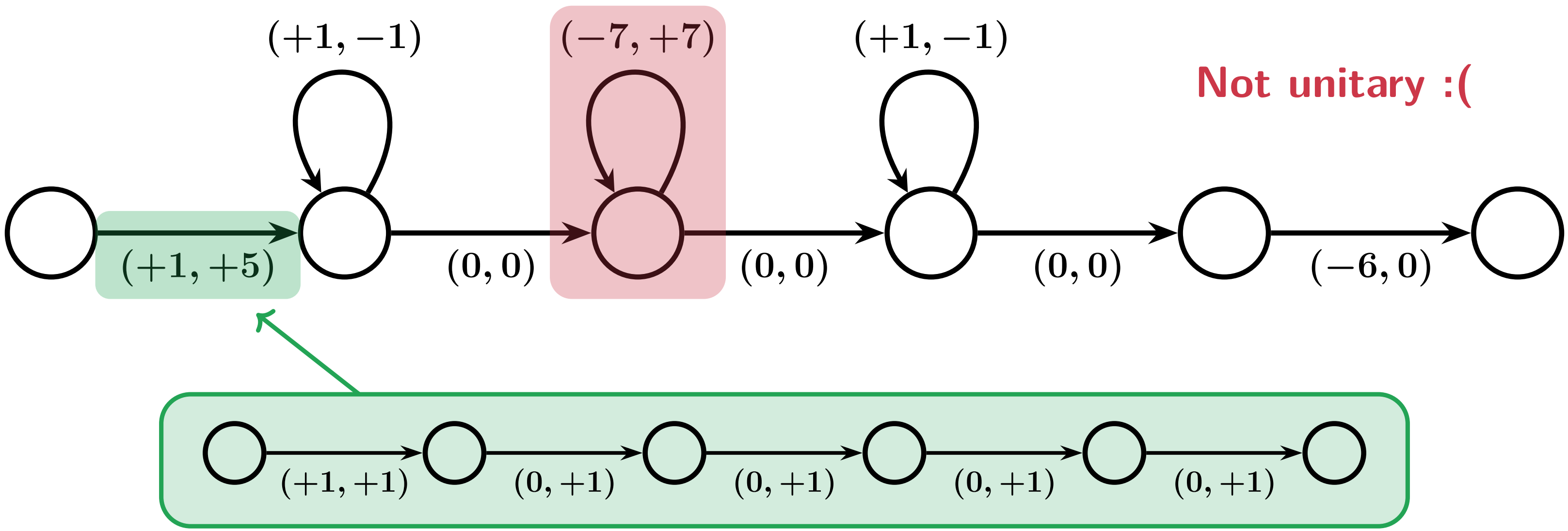
Unitary Simple Linear Path Schemes

Definition (Unitary SLPS)**.** An SLPS where the counter updates are restricted to $\{-1, 0, +1\}$.



Unitary Simple Linear Path Schemes

Definition (Unitary SLPS)**.** An SLPS where the counter updates are restricted to $\{-1, 0, +1\}$.



Reachability in Unitary SLPS

Theorem 3. Reachability in unitary inverse-Ackermann-dimensional SLPS is NP-complete.

UnitaryInverseAckermannDimensionalSimpleLinearPathSchemeReachability

`Input:` a natural number k encoded in unary,

a unitary SLPS $\mathcal{V}$ of dimension $\mathcal{O}(\alpha(k))$ and size $\textit{\textbf{poly}}(k)$,

an initial configuration $p(u)$ encoded in unary, and

a target configuration $q(v)$ encoded in unary.

`Question:` is there a run from $p(u)$ to $q(v)$ in $\mathcal{V}$?

Notation: $\alpha : \mathbb{N} \to \mathbb{N}$ is the inverse Ackermann function.

Reachability in Unitary SLPS

Theorem 3. Reachability in unitary inverse-Ackermann-dimensional SLPS is NP-complete.

UnitaryInverseAckermannDimensionalSimpleLinearPathSchemeReachability

`Input:` a natural number k encoded in unary,
a unitary SLPS $\mathcal{V}$ of dimension $\mathcal{O}(\alpha(k))$ and size $\textit{\textbf{poly}}(k)$,
an initial configuration $p(u)$ encoded in unary, and
a target configuration $q(v)$ encoded in unary.

`Question:` is there a run from $p(u)$ to $q(v)$ in $\mathcal{V}$?

Proof ingredients. 3-SAT reduction. Chinese remainder encoding for SAT.
Conjunction of non-divisibility assertions.
Unitary 5-SLPS with zero tests for asserting non-divisibility.
Concatenate non-divisibility asserting unitary SLPSs. *Simulate zero tests with a different technique.*

Notation: $\alpha : \mathbb{N} \to \mathbb{N}$ is the inverse Ackermann function.

Recap of Main Results

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Theorem 2. Reachability in unary ultraflat 4-VASS is NP-complete.

Open problem. Is reachability in unary ultraflat 3-VASS NP-complete?

Theorem 3. Reachability in unitary inverse-Ackermann-dimensional SLPS is NP-complete.

Open problem. Does there exist $\boldsymbol{d} \in \mathbb{N}$ such that reachability in unitary $\boldsymbol{d}$-SLPS is NP-complete?

Theorem 4. Reachability in unary 2-SLPS with binary encoded initial and target configurations is in P.

Recap of Main Results

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Theorem 2. Reachability in unary ultraflat 4-VASS is NP-complete.

Open problem. Is reachability in unary ultraflat 3-VASS NP-complete?

Theorem 3. Reachability in unitary inverse-Ackermann-dimensional SLPS is NP-complete.

Open problem. Does there exist $d \in \mathbb{N}$ such that reachability in unitary d-SLPS is NP-complete?

Theorem 4. Reachability in unary 2-SLPS with binary encoded initial and target configurations is in P.

Reachability in Unary Encoded 2-SLPS with Binary Encoded Initial and Target Configurations

Theorem 4. Reachability in unary 2-SLPS with binary encoded initial and target configurations is in P.

`Input:` a natural number $\boldsymbol{k}$ encoded in unary,
a (unary) 2-SLPS $\boldsymbol{\mathcal{V}}$ of size $\boldsymbol{poly(k)}$,
an initial configuration $\boldsymbol{p(u)}$ such that $\boldsymbol{|u[1]|, |u[2]| \leq 2^k}$, and
a target configuration $\boldsymbol{q(v)}$ such that $\boldsymbol{|v[1]|, |v[2]| \leq 2^k}$.

`Question:` is there a run from $\boldsymbol{p(u)}$ to $\boldsymbol{q(v)}$ in $\boldsymbol{\mathcal{V}}$?

Reachability in Unary Encoded 2-SLPS with Binary Encoded Initial and Target Configurations

Theorem 4. Reachability in unary 2-SLPS with binary encoded initial and target configurations is in P.

`Input:` a natural number $\boldsymbol{k}$ encoded in unary,
a (unary) 2-SLPS $\boldsymbol{\mathcal{V}}$ of size $\boldsymbol{poly(k)}$,
an initial configuration $\boldsymbol{p(u)}$ such that $|\boldsymbol{u[1]}|, |\boldsymbol{u[2]}| \leq \boldsymbol{2^k}$, and
a target configuration $\boldsymbol{q(v)}$ such that $|\boldsymbol{v[1]}|, |\boldsymbol{v[2]}| \leq \boldsymbol{2^k}$.

`Question:` is there a run from $\boldsymbol{p(u)}$ to $\boldsymbol{q(v)}$ in $\boldsymbol{\mathcal{V}}$?

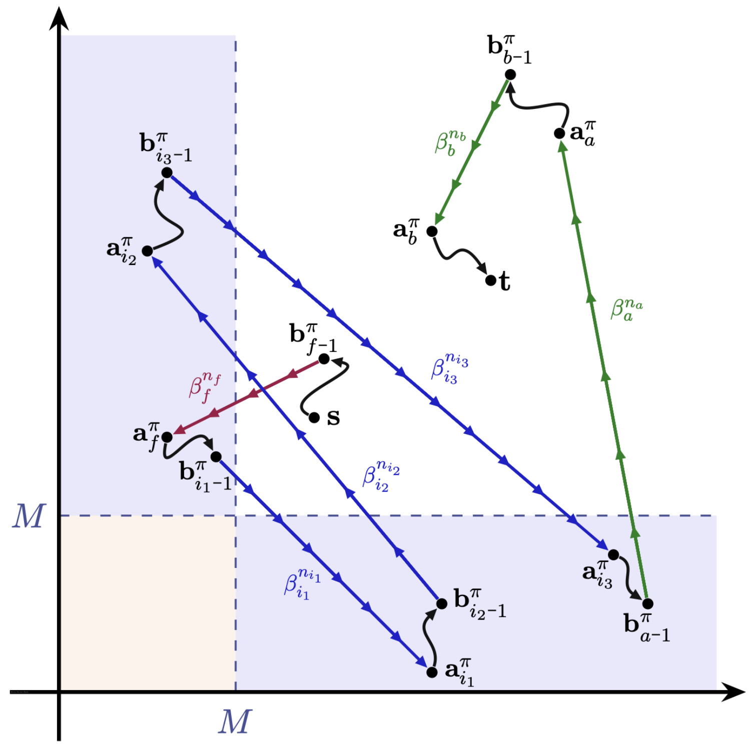
Two proof parts:

(1) Identify a sufficient and *"nice"* collection of reachability witnessing runs.

(2) Explore configurations reachable along such runs using a dynamic programming algorithm.

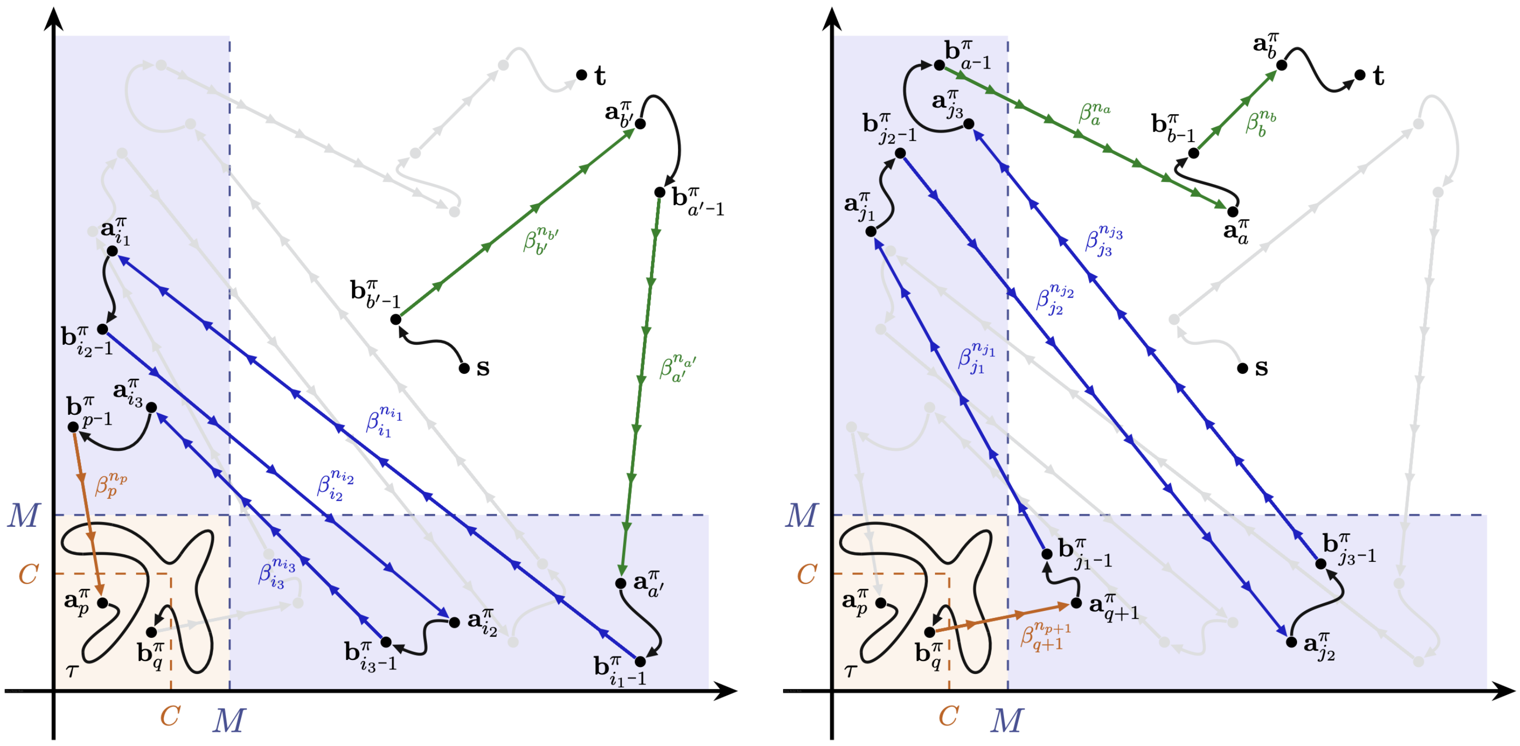
Structural Theorem for Reachability in 2-SLPS

Thm. Let $\mathcal{V}$ be a unary 2-SLPS. There exists $M \leq \textbf{\textit{poly}}(\textbf{\textit{size}}(\mathcal{V}))$ such that whenever $p(s) \xrightarrow{*} q(t)$, there is a path π such that $p(s) \xrightarrow{\pi} q(t)$ and π has *flavour A* or *flavour B*



Structural Theorem for Reachability in 2-SLPS

Thm. Let $\mathcal{V}$ be a unary 2-SLPS. There exists $M \leq \textit{\textbf{poly}}(\textit{\textbf{size}}(\mathcal{V}))$ such that whenever $p(s) \xrightarrow{*} q(t)$, there is a path π such that $p(s) \xrightarrow{\pi} q(t)$ and π has *flavour A* or *flavour B*.



The Tractability Border of Reachability in Simple Vector Addition Systems with States

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Theorem 2. Reachability in unary ultraflat 4-VASS is NP-complete.

Open problem. Is reachability in unary ultraflat 3-VASS NP-complete?

Theorem 3. Reachability in unitary inverse-Ackermann-dimensional SLPS is NP-complete.

Open problem. Does there exist $d \in \mathbb{N}$ such that reachability in unitary d-SLPS is NP-complete?

Theorem 4. Reachability in unary 2-SLPS with *binary encoded initial and target configurations* is in P.

The Tractability Border of Reachability in Simple Vector Addition Systems with States

Theorem 1. Reachability in unary 3-SLPS is NP-complete.

Theorem 2. Reachability in unary ultraflat 4-VASS is NP-complete.

Open problem. Is reachability in unary ultraflat 3-VASS NP-complete?

Theorem 3. Reachability in unitary inverse-Ackermann-dimensional SLPS is NP-complete.

Open problem. Does there exist $d \in \mathbb{N}$ such that reachability in unitary d-SLPS is NP-complete?

Theorem 4. Reachability in unary 2-SLPS with *binary encoded initial and target configurations* is in P.

Thank You!

Presented by Henry Sinclair-Banks, University of Warsaw, Poland

UNIVERSITY OF LIVERPOOL

Verification Seminar, University of Liverpool, UK

Presentation made with BeamerikZ

Ultraflat 3-VASS with Zero Tests for Asserting Non-Divisibility

```
LOOP: x += 1, y += 5, z −= 1
LOOP: x += 2, y += 6, z −= 1
LOOP: x += 3, y += 7, z −= 1
LOOP: x += 4, y += 8, z −= 1
zero-test(z)
LOOP: x −= 5, z += 5
zero-test(x)
LOOP: x += 1, z −= 1
zero-test(z)
LOOP: x −= 1, y −= 5, z += 1
LOOP: x −= 2, y −= 6, z += 1
LOOP: x −= 3, y −= 7, z += 1
LOOP: x −= 4, y −= 8, z += 1
zero-test(y)
```

Suppose we want to assert $\mathbf{5} \nmid \boldsymbol{v}$.

This ultraflat 3-VASS with zero tests:

- starts with $\mathsf{x} = \boldsymbol{v}$, $\mathsf{y} = \mathbf{0}$, $\mathsf{z} = \mathbf{1}$,
- can only be passed if $\mathbf{5} \nmid \boldsymbol{v}$, and
- ends with $\mathsf{x} = \boldsymbol{v}$, $\mathsf{y} = \mathbf{0}$, $\mathsf{z} = \mathbf{1}$.

(i) Choose $\boldsymbol{r} \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}\}$ ...

(ii) ... such that $\mathbf{5} \mid \boldsymbol{v} + \boldsymbol{r}$.

(iii) Restore $\mathsf{x} = \boldsymbol{v}$, $\mathsf{y} = \mathbf{0}$.