Rational Loop Synthesis

Anton Varonka

TU WIEN Informatics

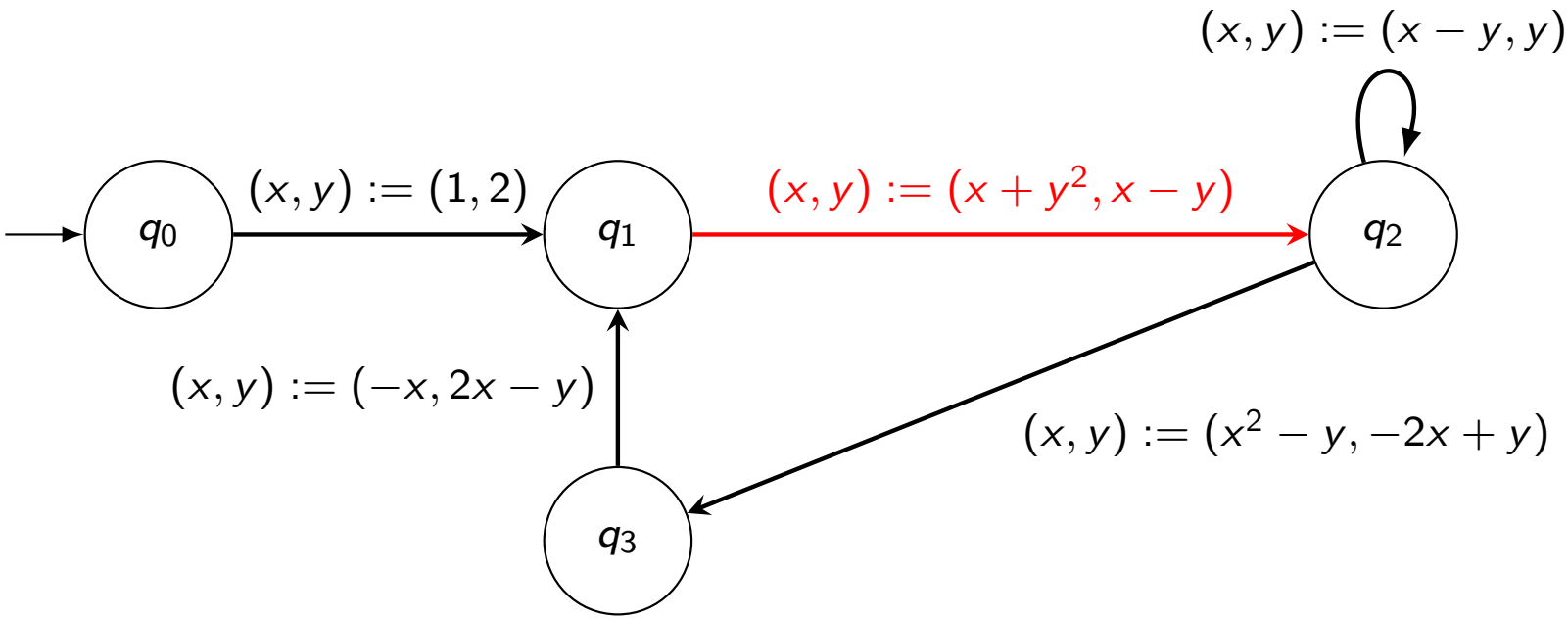
based on joint work with

many great researchers

The project leading to this work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101034440.

Loop Invariants and Algebraic Reasoning
Aarhus, Denmark
July 7th, 2025

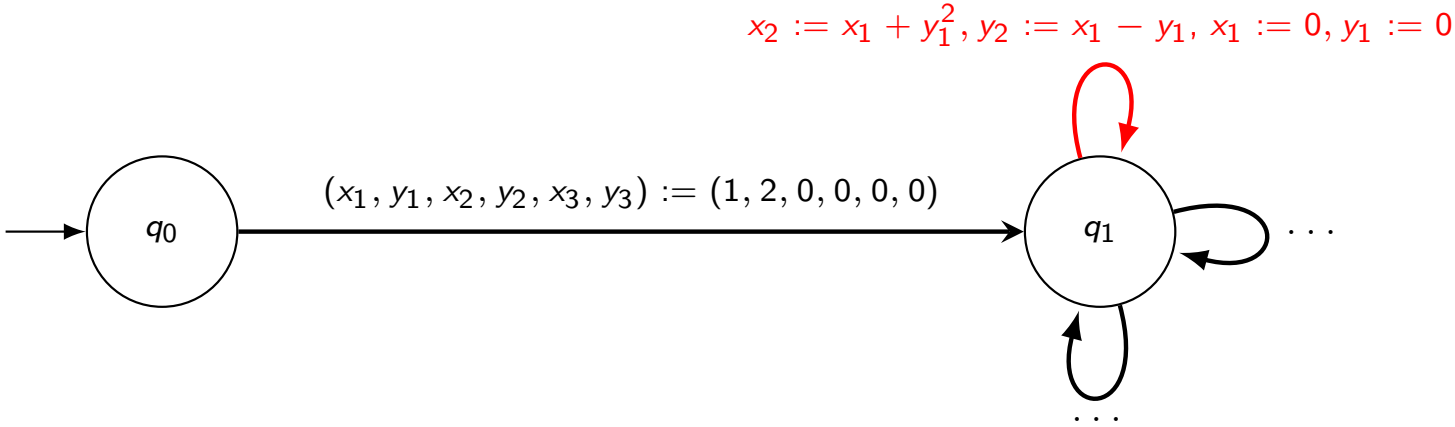
Polynomial Programs



ℓ non-initial locations, d variables

Goal: understand the reachable sets in $\mathbb{Q}^d$

Polynomial Loops



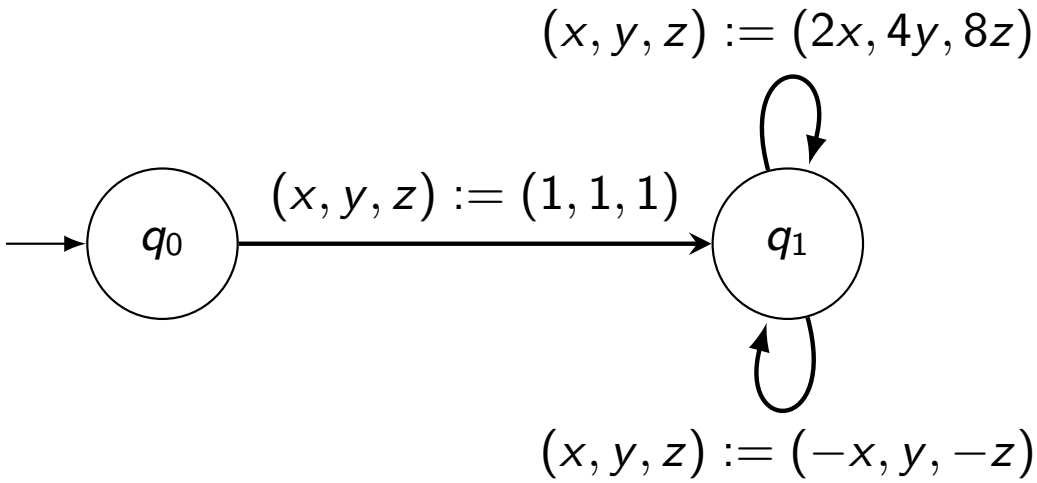
After reduction: $\ell \cdot d$ variables & same type of updates
Non-determinism, or "multi-path" loops

Focus on the set $S \subseteq \mathbb{Q}^{\ell d}$ of vectors reachable in q_1

Algebraic Invariants

an algebraic set

is a subset $V \subseteq \overline{\mathbb{Q}}^d$ defined by polynomial equalities.

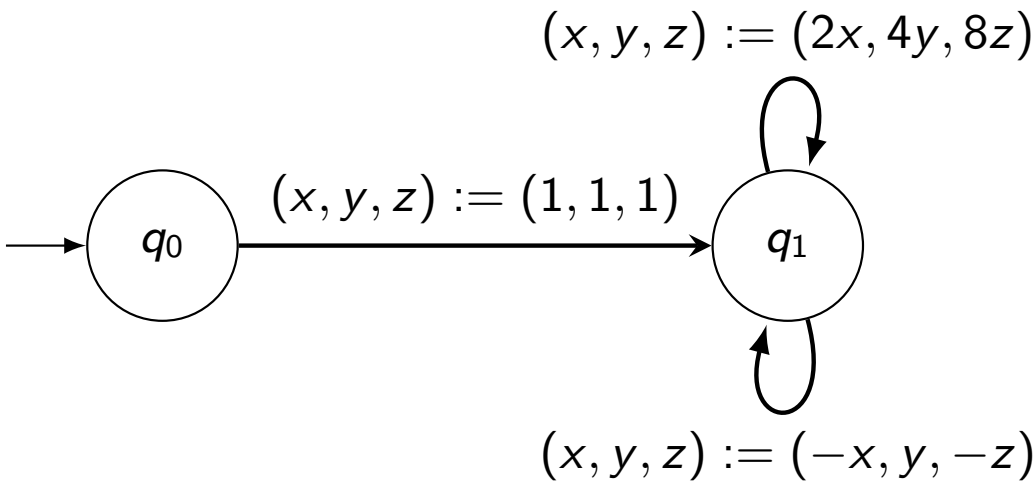


An algebraic set can overapproximate the reachable set S,
e.g., $S \subseteq V(\, x^2 - y \,)$. Then we call V an algebraic invariant of the loop.

Strongest Algebraic Invariant

Zariski closure $\overline{S}$ is the smallest algebraic set containing S.

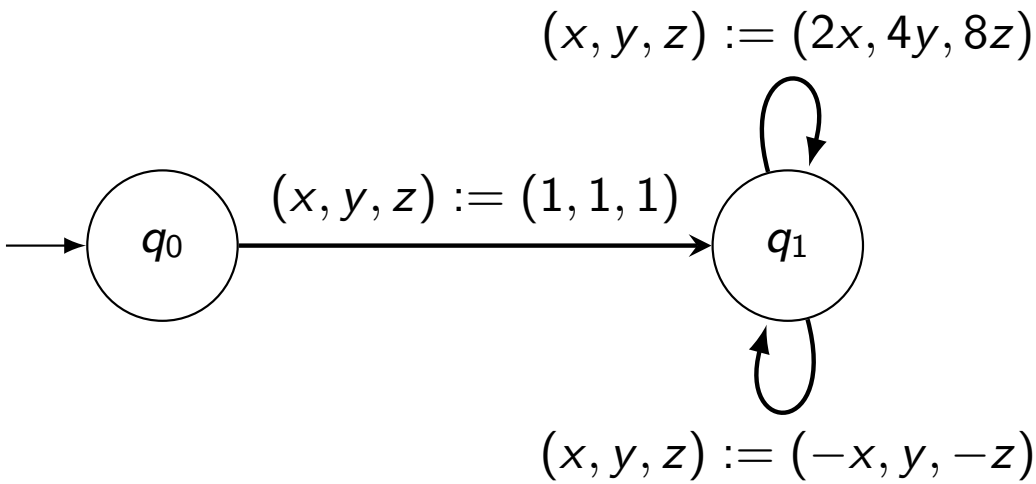
smallest algebraic set $\leftrightarrow$ strongest algebraic invariant



Strongest Algebraic Invariant

Zariski closure $\overline{S}$ is the smallest algebraic set containing S.

smallest algebraic set $\leftrightarrow$ strongest algebraic invariant



always a zero set of a finite collection of polynomials $\rightarrow$ finitary object

$$\overline{S} = V(\, x^2 - y, x^3 - z \,)$$

Beyond Linear Loops

Theorem [Kovács, V.] RAMiCS'23

The strongest algebraic invariant of a multi-path loop with polynomial updates of degree ≤ 2 is algorithmically **uncomputable**.

Reduction from the Boundedness Problem for Reset VASS.

Theorem [Müllner, Moosbrugger, Kovács] POPL'24

Computing the strongest algebraic invariant of a single-path polynomial loop is at least **as hard as Skolem problem**.

Open problem 1: Is it uncomputable?

Linear Loops

Thm. [Hrushovski, Ouaknine, Pouly, Worrell] LICS'18

The strongest algebraic invariant of a multi-path linear loop can be computed.

But what ARE the polynomials?

Linear Loops

Thm. [Hrushovski, Ouaknine, Pouly, Worrell] LICS'18

The strongest algebraic invariant of a multi-path linear loop can be computed.

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.] POPL'25

The strongest algebraic invariant of a single-path linear loop can be computed in polynomial time.

$\boldsymbol{x} := \boldsymbol{s} \in \mathbb{Q}^d$
while $\star$ **do**
  $\boldsymbol{x} := M \cdot \boldsymbol{x}$

But what ARE the polynomials?

Linear Loops

Thm. [Hrushovski, Ouaknine, Pouly, Worrell] LICS'18

The strongest algebraic invariant of a multi-path linear loop can be computed.

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.] POPL'25

The strongest algebraic invariant of a single-path linear loop can be computed in polynomial time.

$\boldsymbol{x} := \boldsymbol{s} \in \mathbb{Q}^d$
while $\star$ **do**
  $\boldsymbol{x} := M \cdot \boldsymbol{x}$

Based on a polynomial-time procedure to compute multiplicative relations of M's eigenvalues.

But what ARE the polynomials?

Loop invariants: reverse engineering

$(x, y) := (0, 0)$
while $y < N$ **do**
  $x := x + 2y + 1$
  $y := y + 1$

??
holds before and
after each iteration

Loop invariants: reverse engineering

$(x, y) := (0, 0)$
while $y < N$ **do**
  $x := x + 2y + 1$
  $y := y + 1$

??
holds before and
after each iteration

$$(0,0), \quad (1,1), \quad (4,2), \quad \ldots$$

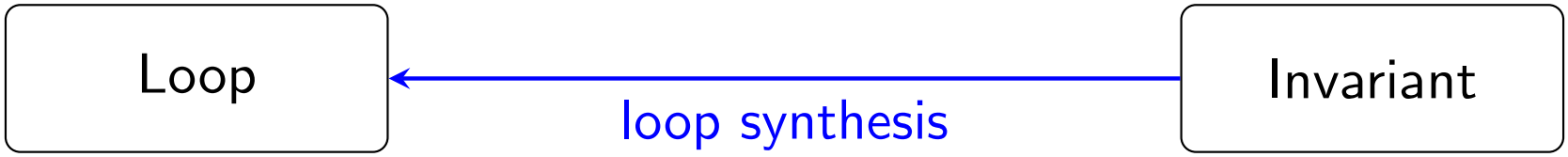
Loop invariants: reverse engineering

$(x, y) := (0, 0)$
while $y < N$ **do**
  $x := x + 2y + 1$
  $y := y + 1$

$y = x^2$
holds before and
after each iteration

$(0, 0), \quad (1, 1), \quad (4, 2), \quad \ldots$

Loop invariants: reverse engineering



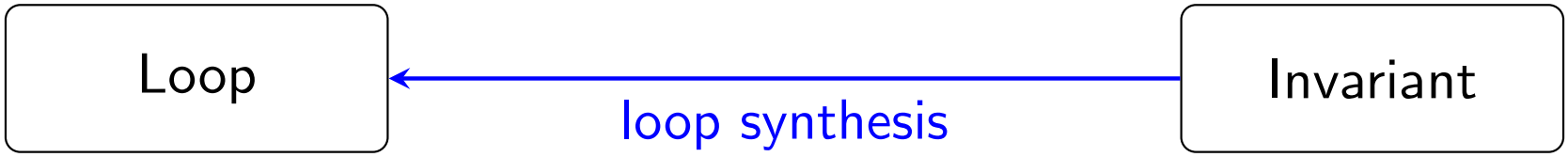
$(x, y) := (0, 0)$
while $y < N$ **do**
  $x := x + 2y + 1$
  $y := y + 1$

$(0,0), \quad (1,1), \quad (4,2), \quad \ldots$

$y = x^2$
holds before and
after each iteration

For a polynomial invariant $p = 0$, synthesise a correct linear loop.

Loop invariants: reverse engineering



$(x, y) := (0, 0)$
while $y < N$ **do**
  $x := x + 2y + 1$
  $y := y + 1$

$y = x^2$
holds before and
after each iteration

$(0, 0), \quad (1, 1), \quad (4, 2), \quad \ldots$

For a polynomial invariant $p = 0$, synthesise a correct linear loop.

Decide whether such a loop exists.

Loop Synthesis problem

Given: a finite set of polynomials S
defining an algebraic set $V(S) \subseteq \overline{\mathbb{Q}}^d$,

Loop Synthesis problem

Given: a finite set of polynomials S defining an algebraic set $V(S) \subseteq \overline{\mathbb{Q}}^d$,

decide whether there exist:

- an update matrix $M \in \mathbb{Q}^{d \times d}$,
- initial vector $\boldsymbol{s} \in \mathbb{Q}^d$,

Is there a loop?

$\boldsymbol{x} := \boldsymbol{s}$;

while $\star$ **do**

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} := M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix};$$

Loop Synthesis problem

Given: a finite set of polynomials S
defining an algebraic set $V(S) \subseteq \overline{\mathbb{Q}}^d$,

decide whether there exist:

- an update matrix $M \in \mathbb{Q}^{d \times d}$,
- initial vector $\boldsymbol{s} \in \mathbb{Q}^d$,

such that

$$\mathcal{O} = \{\boldsymbol{s}, M\boldsymbol{s}, M^2\boldsymbol{s}, \dots\} \subseteq V(S) \quad \text{[weak]}$$

or

$$\overline{\mathcal{O}} = \{\boldsymbol{s}, M\boldsymbol{s}, M^2\boldsymbol{s}, \dots\} = V(S) \quad \text{[strong]}$$

Is there a loop?

$\boldsymbol{x} := \boldsymbol{s}$;
while $\star$ **do**

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} := M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix};$$

with (strongest)
algebraic invariant $V(S)$

Loop Synthesis problem

Given: a finite set of polynomials S
defining an algebraic set $V(S) \subseteq \overline{\mathbb{Q}}^d$,

decide whether there exist:

- an update matrix $M \in \mathbb{Q}^{d \times d}$,
- initial vector $\boldsymbol{s} \in \mathbb{Q}^d$,

such that

$$\mathcal{O} = \{\boldsymbol{s}, M\boldsymbol{s}, M^2\boldsymbol{s}, \dots\} \subseteq V(S) \quad \text{[weak]}$$

or

$$\overline{\mathcal{O}} = \{\boldsymbol{s}, M\boldsymbol{s}, M^2\boldsymbol{s}, \dots\} = V(S) \quad \text{[strong]}$$

☞ We always search for an infinite orbit $\mathcal{O}$.

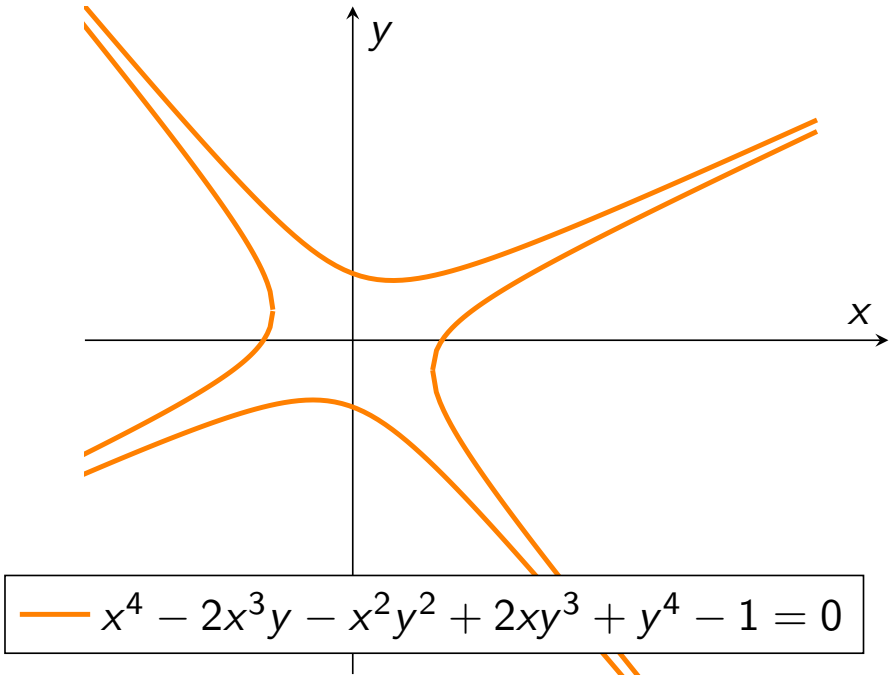
Is there a loop?

$\boldsymbol{x} := \boldsymbol{s}$;
while $\star$ **do**

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} := M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix};$$

with (strongest)
algebraic invariant $V(S)$

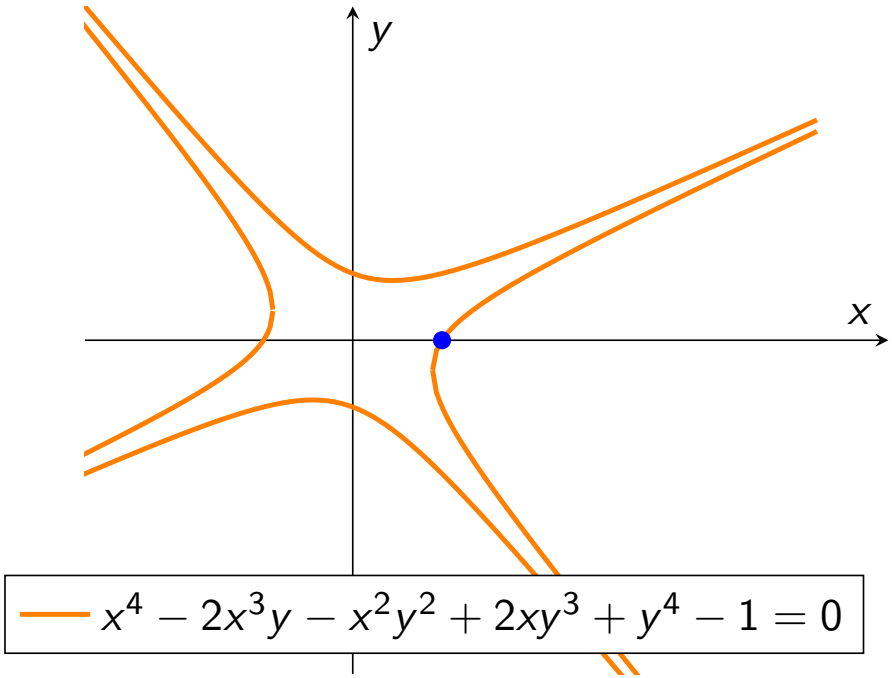
Loop synthesis: (algebra-)geometrically



sample rational points from a variety

☞ We always sample infinitely many points.

Loop synthesis: (algebra-)geometrically



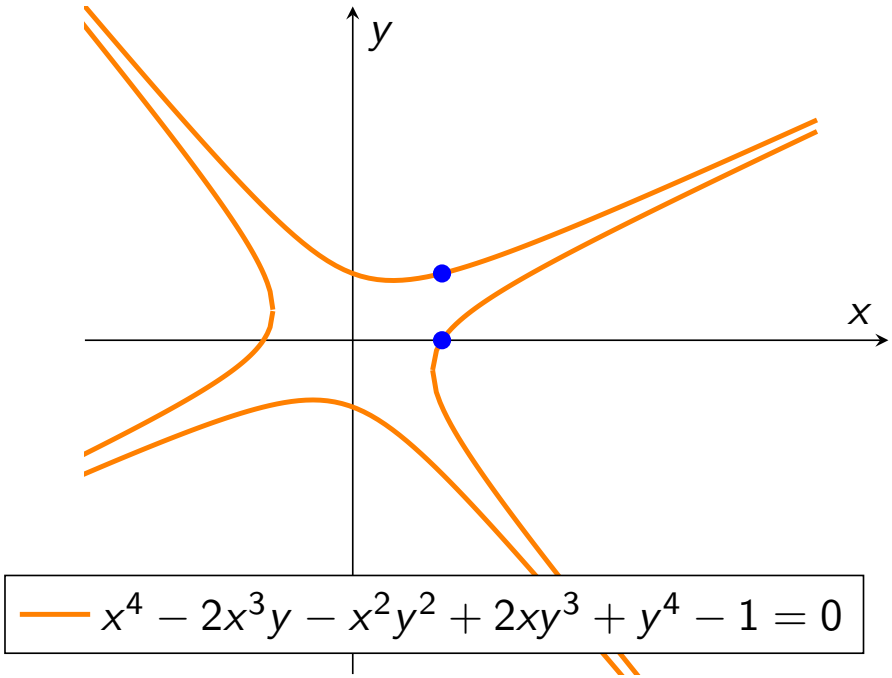
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

sample rational points from a variety

$(x, y) \leftarrow (1, 0);$
while $*$ **do**
  $x \leftarrow x + y;$
  $y \leftarrow x;$

☞ We always sample infinitely many points.

Loop synthesis: (algebra-)geometrically



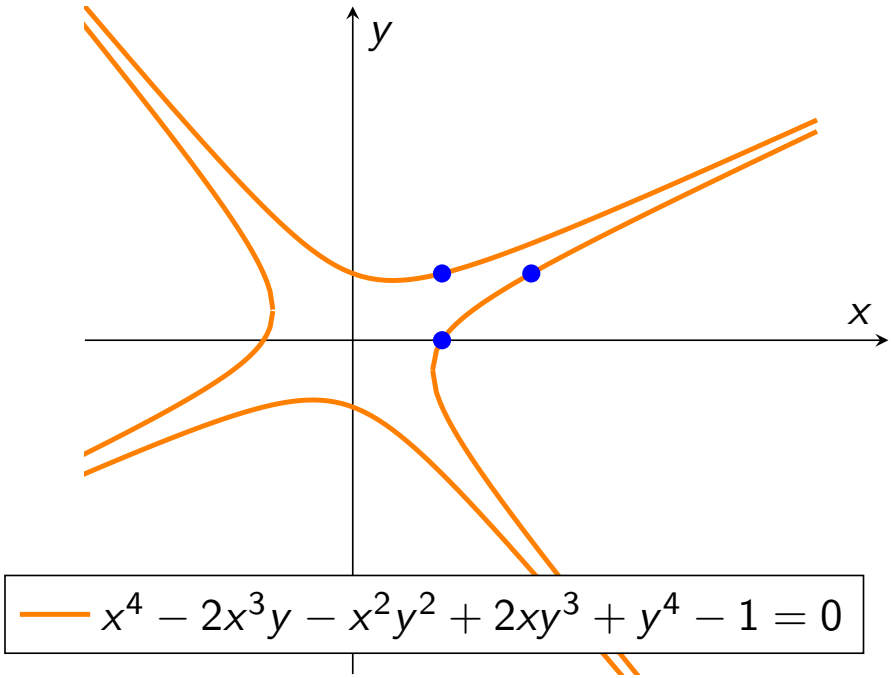
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \ldots$$

sample rational points from a variety

$(x, y) \leftarrow (1, 0);$
while $*$ **do**
  $x \leftarrow x + y;$
  $y \leftarrow x;$

☞ We always sample infinitely many points.

Loop synthesis: (algebra-)geometrically



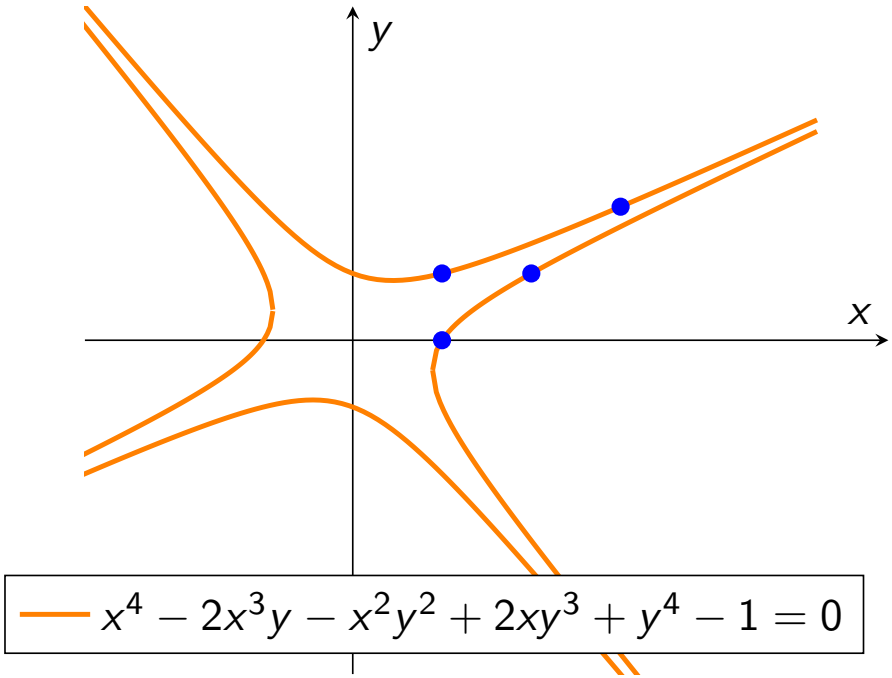
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \ldots$$

sample rational points from a variety

$(x, y) \leftarrow (1, 0);$
while $*$ **do**
  $x \leftarrow x + y;$
  $y \leftarrow x;$

☞ We always sample infinitely many points.

Loop synthesis: (algebra-)geometrically



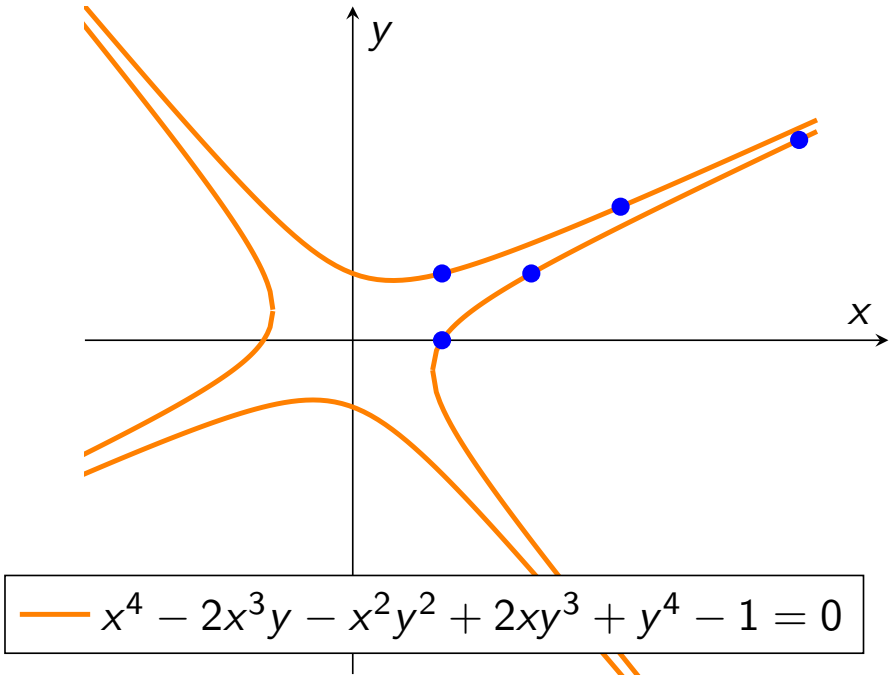
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \ldots$$

sample rational points from a variety

$(x, y) \leftarrow (1, 0);$
while $*$ **do**
  $x \leftarrow x + y;$
  $y \leftarrow x;$

☞ We always sample infinitely many points.

Loop synthesis: (algebra-)geometrically



$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix}, \ldots$$

sample rational points from a variety

$(x, y) \leftarrow (1, 0);$
while $*$ **do**
  $x \leftarrow x + y;$
  $y \leftarrow x;$

☞ We always sample infinitely many points.

Loop Synthesis is hard

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.] POPL'25

The weak synthesis problem over $\{\mathbb{Z}, \mathbb{Q}\}$ is as hard as Hilbert's 10th problem over $\{\mathbb{Z}, \mathbb{Q}\}$.

H10 over $R \in \{\mathbb{Z}, \mathbb{Q}\}$: solve a system of polynomial equations over R.

- undecidable for $R = \mathbb{Z}$,
- decidability open for $R = \mathbb{Q}$.

we encode an H10-instance $\{p_1, \ldots, p_k\}$ as finding a loop with algebraic invariant $V(p_1, \ldots, p_k, p)$

Pure difference binomials

Does an equation $p(x_1, \ldots, x_d) = 0$ have infinitely many solutions in $\mathbb{Q}$?

Pure difference binomials

Does an equation $p(x_1, \ldots, x_d) = 0$ have infinitely many solutions in $\mathbb{Q}$?

– Yes, if p is a **pure difference binomial** (PDB).

Pure difference binomials

Does an equation $p(x_1, \ldots, x_d) = 0$ have infinitely many solutions in $\mathbb{Q}$?

– Yes, if p is a **pure difference binomial** (PDB).

A pure difference binomial is a polynomial $p \in \mathbb{Q}[x_1, \ldots, x_d]$ of the form

$$p = x_1^{\alpha_1} \ldots x_d^{\alpha_d} - x_1^{\beta_1} \ldots x_d^{\beta_d},$$

where $\alpha_i, \beta_i \in \mathbb{N}$ for all $i = 1, \ldots, d$.

Examples in $\mathbb{Q}[x, y, z]$: $1 - xyz$, $xz - y^3$, $x^2y - z^3$, etc.

A Loop for PDBs

Loop Synthesis for PDB ideals

Input: pure difference binomials $p_1, \ldots, p_k$.

Output: A linear loop for which every $p \in I = \langle p_1, \ldots, p_k \rangle$ is invariant.

A Loop for PDBs

Loop Synthesis for PDB ideals

Input: pure difference binomials $p_1, \ldots, p_k$.
Output: A linear loop for which every $p \in I = \langle p_1, \ldots, p_k \rangle$ is invariant.

Theorem [Kenison, Kovács, V.] ISSAC'23

Let $p_1, p_2, \ldots, p_k \in \mathbb{Q}[x_1, \ldots, x_d]$ be PDBs; let $I = \langle p_1, \ldots, p_k \rangle$.

- There exists a linear loop $\mathcal{L} = (M, \boldsymbol{s}) \in \mathbb{Q}^{d \times d} \times \mathbb{Q}^d$ s.t. $V(I)$ is its algebraic invariant.
- An effective procedure constructs $\mathcal{L}$.
- If $k < d$, then $\mathcal{L}$ has an infinite orbit.

Loops for systems of PDBs

We show how to combine multiple pure difference binomials.

$x^2 - y = 0 \wedge x^3 - z = 0 \longrightarrow$ a linear loop with 3 variables.

Loops for systems of PDBs

We show how to combine multiple pure difference binomials.

$x^2 - y = 0 \wedge x^3 - z = 0 \longrightarrow$ a linear loop with 3 variables.

$(x, y, z) := (1, 1, 1);$
while $\star$ **do**

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix};$$

Loops for systems of PDBs

We show how to combine multiple pure difference binomials.

$x^2 - y = 0 \wedge x^3 - z = 0 \longrightarrow$ a linear loop with 3 variables.

$(x, y, z) := (1, 1, 1);$
while $\star$ **do**

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix};$$

$$\begin{aligned} \langle x(n) \rangle_{n=0}^{\infty} &: \quad 1, 2, 4, \ldots \\ \langle y(n) \rangle_{n=0}^{\infty} &: \quad 1, 4, 16, \ldots \\ \langle z(n) \rangle_{n=0}^{\infty} &: \quad 1, 8, 64, \ldots \end{aligned}$$

For n-th terms, it holds: $x(n)^2 - y(n) = 0 \wedge x^3(n) - z(n) = 0$.

Multiplicative Relations

Assume we search for a diagonal matrix $M = \mathrm{diag}(\lambda_1, \ldots, \lambda_d)$.

$(x, y, z) := (x_0, y_0, z_0)$;
while $\star$ **do**

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix};$$

$$\left(\frac{x}{x_0}\right)^2 - \left(\frac{y}{y_0}\right) = (\lambda_1^n)^2 - \lambda_2^n = (2^n)^2 - (4^n) = 0 \textbf{ for all } n.$$

Multiplicative Relations

Assume we search for a diagonal matrix $M = \mathrm{diag}(\lambda_1, \ldots, \lambda_d)$.

$(x, y, z) := (x_0, y_0, z_0)$;
while $\star$ **do**
$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix};$$

$$\left(\frac{x}{x_0}\right)^2 - \left(\frac{y}{y_0}\right) = (\lambda_1^n)^2 - \lambda_2^n = (2^n)^2 - (4^n) = 0 \textbf{ for all } n.$$

A multiplicative relation

of $\lambda_1, \ldots, \lambda_d \in \overline{\mathbb{Q}}$ is a tuple $(v_1, \ldots, v_d) \in \mathbb{Z}^d$ s.t.

$$\lambda_1^{v_1} \ldots \lambda_d^{v_d} = 1.$$

Multiplicative Relations

Assume we search for a diagonal matrix $M = \mathrm{diag}(\lambda_1, \ldots, \lambda_d)$.

$(x, y, z) := (x_0, y_0, z_0)$;
while $\star$ **do**

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix};$$

$$\left(\frac{x}{x_0}\right)^2 - \left(\frac{y}{y_0}\right) = (\lambda_1^n)^2 - \lambda_2^n = (2^n)^2 - (4^n) = 0 \textbf{ for all } n.$$

A multiplicative relation

of $\lambda_1, \ldots, \lambda_d \in \overline{\mathbb{Q}}$ is a tuple $(v_1, \ldots, v_d) \in \mathbb{Z}^d$ s.t.

$$\lambda_1^{v_1} \ldots \lambda_d^{v_d} = 1.$$

polynomials vanishing on $(\lambda_1^n, \ldots, \lambda_d^n)$ for all n
are generated by PDBs of multiplicative relations of $\lambda_1, \ldots, \lambda_d$

Multiplicative Relations

Assume we search for a diagonal matrix $M = \mathrm{diag}(\lambda_1, \ldots, \lambda_d)$.

$(x, y, z) := (x_0, y_0, z_0)$;
while $\star$ **do**

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix};$$

$$\left(\frac{x}{x_0}\right)^2 - \left(\frac{y}{y_0}\right) = (\lambda_1^n)^2 - \lambda_2^n =$$
$$(2^n)^2 - (4^n)^1 = 0 \textbf{ for all } n.$$

$(2, -1)$ is a mult. rel.

A multiplicative relation

of $\lambda_1, \ldots, \lambda_d \in \overline{\mathbb{Q}}$ is a tuple $(v_1, \ldots, v_d) \in \mathbb{Z}^d$ s.t.

$$\lambda_1^{v_1} \ldots \lambda_d^{v_d} = 1.$$

polynomials vanishing on $(\lambda_1^n, \ldots, \lambda_d^n)$ for all n
are generated by PDBs of multiplicative relations of $\lambda_1, \ldots, \lambda_d$

Quadratic Invariants

Avoiding hardness of Hilbert's 10: bound the degree of polynomials.

Quadratic Invariants

Avoiding hardness of Hilbert's 10: bound the degree of polynomials.

Thm. [Grunewald & Segal] (1981)

There is an algorithm to decide whether a quadratic equation in arbitrary number of variables has a rational solution.

$$\frac{3}{2} \cdot x^2 - 7 \cdot xy + \frac{4}{3} \cdot xz - z^2 + 31 \cdot y + z - 7 = 0$$

Quadratic Invariants

Avoiding hardness of Hilbert's 10: bound the degree of polynomials.

Thm. [Grunewald & Segal] (1981)

There is an algorithm to decide whether a quadratic equation in arbitrary number of variables has a rational solution.

$$\frac{3}{2} \cdot x^2 - 7 \cdot xy + \frac{4}{3} \cdot xz - z^2 + 31 \cdot y + z - 7 = 0$$

But: we still need to find a matrix M.

Consider an equation $Q(\boldsymbol{x}) = c$,

Q is a quadratic form (homogeneous).

$$x^2 + y^2 - z^2 = 0$$

$(x, y, z) := (3, 4, 5);$
while $\star$ **do**
  $x := 2x;$
  $y := 2y;$
  $z := 2z;$

$(x, y, z) := (3, 4, 5);$
while $\star$ **do**
  $x := x - 2y + 2z;$
  $y := 2x - y + 2z;$
  $z := 2x - 2y + 3z;$

Consider an equation $Q(\boldsymbol{x}) = c$,

Q is a quadratic form (homogeneous).

$$x^2 + y^2 - z^2 = \cancel{0}1$$

$(x, y, z) := (3, 4, 5);$
while $\star$ **do**
  $x := 2x;$
  $y := 2y;$
  $z := 2z;$

$(x, y, z) := (3, 4, 5);$
while $\star$ **do**
  $x := x - 2y + 2z;$
  $y := 2x - y + 2z;$
  $z := 2x - 2y + 3z;$

Consider an equation $Q(\boldsymbol{x}) = c$,

Q is a quadratic form (homogeneous).

$$x^2 + y^2 - z^2 = \cancel{0}1$$

$(x, y, z) := (\mathbf{1}, \mathbf{1}, \mathbf{1})$;
while $\star$ **do**
  $x := 2x$;
  $y := 2y$;
  $z := 2z$;

$(x, y, z) := (\mathbf{1}, \mathbf{1}, \mathbf{1})$;
while $\star$ **do**
  $x := x - 2y + 2z$;
  $y := 2x - y + 2z$;
  $z := 2x - 2y + 3z$;

Consider an equation $Q(\boldsymbol{x}) = c$,

Q is a quadratic form (homogeneous).

$$x^2 + y^2 - z^2 = 1$$

$(x, y, z) := (1, 1, 1);$
while $\star$ **do**
  $x := 2x;$
  $y := 2y;$
  $z := 2z;$

$(x, y, z) := (\mathbf{1}, \mathbf{1}, \mathbf{1});$
while $\star$ **do**
  $x := x - 2y + 2z;$
  $y := 2x - y + 2z;$
  $z := 2x - 2y + 3z;$

$(1, 1, 1) \rightarrow (1, 3, 3) \rightarrow (1, 5, 5) \rightarrow$
$\ldots$ a non-trivial loop!

Consider an equation $Q(\boldsymbol{x}) = c$,

Q is a quadratic form (homogeneous).

$$x^2 + y^2 - z^2 = 1$$

$(x, y, z) := (1, 1, 1);$
while $\star$ **do**
  $x := 2x;$
  $y := 2y;$
  $z := 2z;$

$(x, y, z) := (\mathbf{1}, \mathbf{1}, \mathbf{1});$
while $\star$ **do**
  $x := x - 2y + 2z;$
  $y := 2x - y + 2z;$
  $z := 2x - 2y + 3z;$

$(1, 1, 1) \to (1, 3, 3) \to (1, 5, 5) \to$
$\ldots$ a non-trivial loop!

How did we find this M?

Pell's equation

Intuition: $x^2 - 7y^2 = 1$ has a fundamental solution $(8, 3)$.

Pell's equation

Intuition: $x^2 - 7y^2 = 1$ has a fundamental solution $(8, 3)$.

A loop for $Q = 1$:

while $\star$ **do**
$x := 8x + 3 \cdot 7y;$
$y := 3x + 8y;$

Pell's equation

Intuition: $x^2 - 7y^2 = 1$ has a fundamental solution $(8, 3)$.

A loop for $Q = 1$:

$(x, y) := (\mathbf{8}, \mathbf{3})$;
while $\star$ **do**
  $x := 8x + 21y$;
  $y := 3x + 8y$;

Pell's equation

Intuition: $x^2 - 7y^2 = 1$ has a fundamental solution $(8, 3)$.

A loop for $Q = 1$:

$(x, y) := (\mathbf{8}, \mathbf{3})$;
while $\star$ **do**
  $x := 8x + 21y$;
  $y := 3x + 8y$;

A loop for $Q = 2$:

$(x, y) := (\mathbf{3}, \mathbf{1})$;
while $\star$ **do**
  $x := 8x + 21y$;
  $y := 3x + 8y$;

A loop for $Q = -12$:

$(x, y) := (\mathbf{4}, \mathbf{2})$;
while $\star$ **do**
  $x := 8x + 21y$;
  $y := 3x + 8y$;

Theorem [Kenison, Kovács, Singh, V.] STACS'24

There exists a procedure that, given an equation $Q(x_1, \ldots, x_d) = c$, where Q is a quadratic form, decides whether **a non-trivial linear loop** satisfying it exists and, if so, synthesises a loop.

Arbitrary quadratic equations

Q is a quadratic form, L is a linear form of $\boldsymbol{x} = (x_1, \ldots, x_d)$.

Theorem [Kenison, Kovács, Singh, V.] STACS'24

There exists a procedure that, given an equation $Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c$, decides whether **a non-trivial affine loop** satisfying it exists and, if so, synthesises a loop.

Arbitrary quadratic equations

Q is a quadratic form, L is a linear form of $\boldsymbol{x} = (x_1, \ldots, x_d)$.

Theorem [Kenison, Kovács, Singh, V.] STACS'24

There exists a procedure that, given an equation $Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c$, decides whether **a non-trivial affine loop** satisfying it exists and, if so, synthesises a loop.

$$x^2 + y^2 - 3x - y = 0$$

$(x, y) := (2, -1)$
while $\star$ **do**
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 3/5x - 4/5y + 1 \\ 4/5x + 3/5y - 1 \end{pmatrix}$$

Arbitrary quadratic equations

Q is a quadratic form, L is a linear form of $\boldsymbol{x} = (x_1, \ldots, x_d)$.

Theorem [Kenison, Kovács, Singh, V.] STACS'24

There exists a procedure that, given an equation $Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c$, decides whether **a non-trivial affine loop** satisfying it exists and, if so, synthesises a loop.

$x^2 + y^2 - 3x - y = 0$

$(x, y) := (2, -1)$
while $\star$ **do**
$$\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 3/5x - 4/5y + 1 \\ 4/5x + 3/5y - 1 \end{pmatrix}$$

NB: affine loops in d variables are linear loops in $d + 1$ variables:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 3/5 & -4/5 & 1 \\ 4/5 & 3/5 & -1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

INVARIANTS WITHOUT LOOPS

Some polynomials need an additional variable.

There exists no (non-trivial) linear loop with 2 variables s.t. $x^2 + y^2 - 3x - y = 0$.

INVARIANTS WITHOUT LOOPS

Some polynomials need an additional variable.

There exists no (non-trivial) linear loop with 2 variables s.t. $x^2 + y^2 - 3x - y = 0$.

(alternative loop synthesis question:) given $I \subseteq \mathbb{Q}[x_1, \ldots, x_d]$, does there exist a loop $(M, \boldsymbol{s}) \in \mathbb{Q}^{k \times k} \times \mathbb{Q}^k$ for some $k \geq d$ s.t. $\mathcal{O} \subseteq V(I)$? Here $V(I) \subseteq \overline{\mathbb{Q}}^k$.

Open problem 2: is there an upper bound on k?

Bit-bounded version

Loop synthesis problem: is there a loop with algebraic invariant $V(S)$?
with additional input: integer B.
Search for $\langle M, \boldsymbol{s} \rangle$ with entries of bitsize $\leq B$, call them bit-bounded loops.

Bit-bounded version

Loop synthesis problem: is there a loop with algebraic invariant $V(S)$?
with additional input: integer B.
Search for $\langle M, \boldsymbol{s} \rangle$ with entries of bitsize $\leq B$, call them bit-bounded loops.

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.] POPL'25

- ☞ The strong and weak synthesis problems for bit-bounded loops can be solved with polynomial space.
- ☞ Both versions are NP-hard under appropriate reductions.

Bit-bounded version

Loop synthesis problem: is there a loop with algebraic invariant $V(S)$?
with additional input: integer B.
Search for $\langle M, \boldsymbol{s} \rangle$ with entries of bitsize $\leq B$, call them bit-bounded loops.

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.]
POPL'25

- ☞ The strong and weak synthesis problems for bit-bounded loops can be solved with polynomial space.
- ☞ Both versions are NP-hard under appropriate reductions.

- guess M and $\boldsymbol{s}$ while respecting the bound (**NP**)

Bit-bounded version

Loop synthesis problem: is there a loop with algebraic invariant $V(S)$?
with additional input: integer B.
Search for $\langle M, \boldsymbol{s} \rangle$ with entries of bitsize $\leq B$, call them bit-bounded loops.

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.]
POPL'25

- ☞ The strong and weak synthesis problems for bit-bounded loops can be solved with polynomial space.
- ☞ Both versions are NP-hard under appropriate reductions.

- guess M and $\boldsymbol{s}$ while respecting the bound (**NP**)
- use invariant generation routine for $(M, \boldsymbol{s})$ (**PSPACE**, or **P**)

Bit-bounded version

Loop synthesis problem: is there a loop with algebraic invariant $V(S)$?
with additional input: integer B.
Search for $\langle M, \boldsymbol{s} \rangle$ with entries of bitsize $\leq B$, call them bit-bounded loops.

Thm. [Ait El Manssour, Kenison, Shirmohammadi, V.] POPL'25

- ☞ The strong and weak synthesis problems for bit-bounded loops can be solved with polynomial space.
- ☞ Both versions are NP-hard under appropriate reductions.

- guess M and $\boldsymbol{s}$ while respecting the bound (**NP**)
- use invariant generation routine for $(M, \boldsymbol{s})$ (**PSPACE**, or **P**)
- radical membership test to verify if $\overline{\mathcal{O}} \subseteq V(S)$ (**AM**)

More on bit-bounded

NP-hardness of the weak synthesis: reduce from 3SAT.
$\Phi = C_1 \wedge \cdots \wedge C_m$ with m clauses and d variables $y_1, \ldots, y_d$.

- add $x_i(1 - x_i)$ for each y_i to the polynomial collection S
- for each clause, say $C_i = y_1 \vee \neg y_2 \vee y_d$, add a polynomial p_i, here $(1 - x_1)x_2(1 - x_d)$.

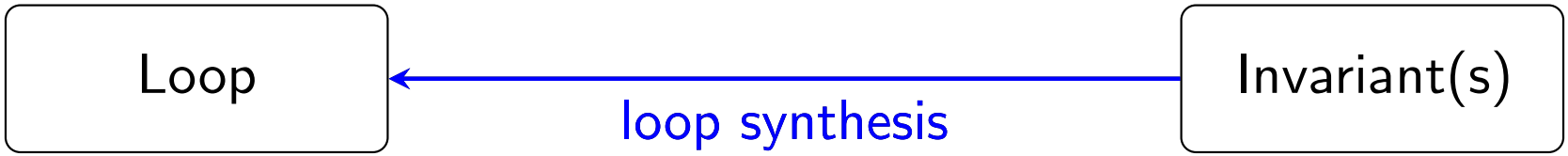
A non-trivial loop $M = \mathrm{diag}(1, \ldots, 1, 2, 2)$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d, 1, 1)$ has invariant $V(S) \Leftrightarrow \exists(\alpha_1, \ldots, \alpha_d)$, a sat. assignment

Open problem 3: Exact complexity of bit-bounded synthesis?

Open Problems

1. Is the strongest algebraic invariant of a single-path polynomial loop uncomputable?
2. Is there an upper bound on the minimal number of variables in a loop that has a given algebraic invariant?
3. What is the exact complexity of the bit-bounded synthesis problem?

Thank you ! Questions ?



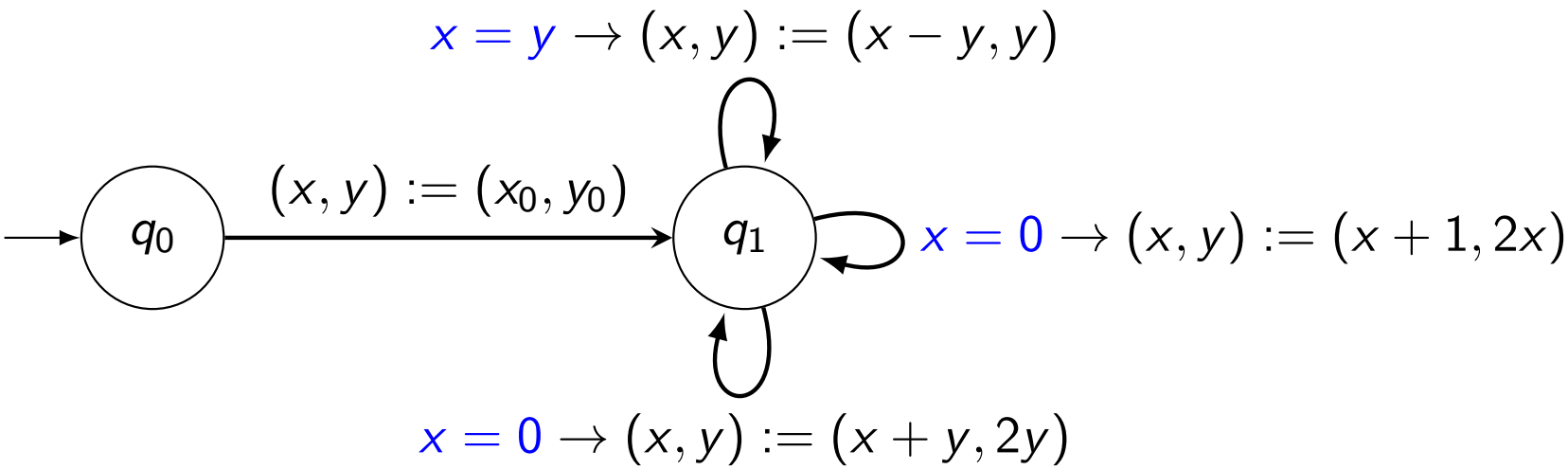
Procedures to synthesise simple (single-path) linear loops for

- invariant ideals generated by pure difference binomials $\rightarrow$ linear loops
- invariants defined by quadratic form equations $\rightarrow$ linear loops
- arbitrary quadratic equations $\rightarrow$ affine loops
- bit-bounded synthesis in **PH** and **NP**-hard

What Else is Unsolvable?

Proposition

Finding the strongest algebraic invariant of a multi-path affine loop with guarded affine updates is algorithmically **unsolvable**.



Multiple quadratic equations

- Loop synthesis for a **system** of quadratic equations: not within reach.

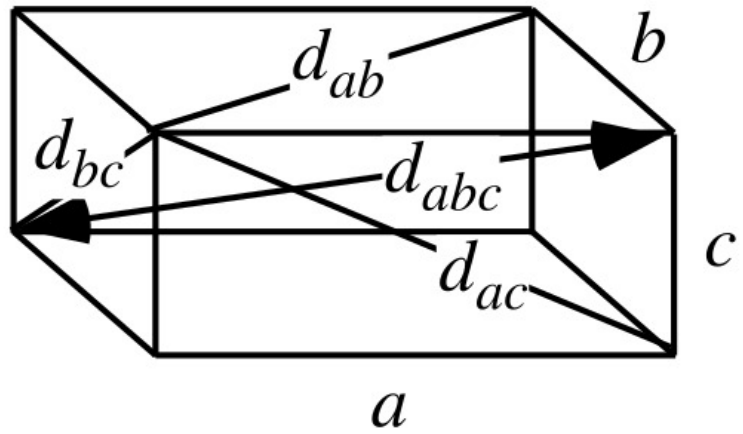
Multiple quadratic equations

- Loop synthesis for a **system** of quadratic equations: not within reach.
- A polynomial equation of any degree can be written as a system of linear and quadratic equations.

Multiple quadratic equations

- Loop synthesis for a **system** of quadratic equations: not within reach.
- A polynomial equation of any degree can be written as a system of linear and quadratic equations.
- **Perfect Euler brick**: a cuboid with edges and all four diagonals of integer length.

$$a^2 + b^2 = d_{ab}^2$$
$$b^2 + c^2 = d_{bc}^2$$
$$c^2 + a^2 = d_{ac}^2$$
$$a^2 + b^2 + c^2 = d_{abc}^2$$



Existence of a perfect Euler brick is **open**.

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

- (already of the form $Q = c$)
- to diagonalise, get rid of xy : $x := x + \frac{1}{2}y, y := y \Rightarrow x^2 - \frac{5}{4}y^2 = 1$
- a loop $\begin{pmatrix} 9 & 10 \\ 8 & 9 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $x^2 - \frac{5}{4}y^2 = 1$

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

- (already of the form $Q = c$)
- to diagonalise, get rid of xy : $x := x + \frac{1}{2}y, y := y \Rightarrow x^2 - \frac{5}{4}y^2 = 1$
- a loop $\begin{pmatrix} 9 & 10 \\ 8 & 9 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $x^2 - \frac{5}{4}y^2 = 1$

Result: a loop $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

- (already of the form $Q = c$)
- to diagonalise, get rid of xy : $x := x + \frac{1}{2}y, y := y \Rightarrow x^2 - \frac{5}{4}y^2 = 1$
- a loop $\begin{pmatrix} 9 & 10 \\ 8 & 9 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $x^2 - \frac{5}{4}y^2 = 1$

Result: a loop $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

- (already of the form $Q = c$)
- to diagonalise, get rid of xy : $x := x + \frac{1}{2}y, y := y \Rightarrow x^2 - \frac{5}{4}y^2 = 1$
- a loop $\begin{pmatrix} 9 & 10 \\ 8 & 9 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $x^2 - \frac{5}{4}y^2 = 1$

Result: a loop $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 13 \\ 8 \end{pmatrix},$

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

- (already of the form $Q = c$)
- to diagonalise, get rid of xy : $x := x + \frac{1}{2}y, y := y \Rightarrow x^2 - \frac{5}{4}y^2 = 1$
- a loop $\begin{pmatrix} 9 & 10 \\ 8 & 9 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $x^2 - \frac{5}{4}y^2 = 1$

Result: a loop $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 13 \\ 8 \end{pmatrix}, \begin{pmatrix} 233 \\ 144 \end{pmatrix},$$

Favourite sequence example

$$x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4 - 1 = 0$$

is a loop invariant, or $p(x, y) = (x^2 - xy - y^2 - 1) \cdot (x^2 - xy - y^2 + 1) = 0$.

Find a loop for $x^2 - xy - y^2 - 1 = 0$.

- (already of the form $Q = c$)
- to diagonalise, get rid of xy : $x := x + \frac{1}{2}y, y := y \Rightarrow x^2 - \frac{5}{4}y^2 = 1$
- a loop $\begin{pmatrix} 9 & 10 \\ 8 & 9 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ for $x^2 - \frac{5}{4}y^2 = 1$

Result: a loop $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 13 \\ 8 \end{pmatrix}, \begin{pmatrix} 233 \\ 144 \end{pmatrix}, \ldots, \begin{pmatrix} F_{6n+1} \\ F_{6n} \end{pmatrix}, \ldots$$