Generating Polynomial Invariants for Hybrid Systems

Enric Rodríguez-Carbonell
Universitat Politècnica de Catalunya
Barcelona (Spain)

Ashish Tiwari
SRI International
Menlo Park (USA)

Introduction

- It is necessary to verify safety properties of hybrid systems
- Exact reach-set of hybrid systems not computable generally
- **Solution:** overapproximate reachable states $\longrightarrow$

INVARIANTS

Main Results

- Method for finding **all** polynomial equality invariants of linear systems
  - **Best** algebraic overapproximation of the reach set

- Extension to hybrid systems using the abstract interpretation framework

Overview of the Talk

1. **Finding Invariants for Linear Systems**
2. **Abstract Interpretation**
3. **Finding Invariants for Hybrid Systems**
4. **Related Work**
5. **Future Work & Conclusions**

Linear Systems
Problem

- Given a system $\dot{x} = Ax + B$ and a set of initial values $Init$, find polynomials p evaluating to 0 at all reachable points
- $\Phi(x^*, t)$ $\equiv$ solution to $\dot{x} = Ax + B$ with initial condition x^*

$$\forall x^* \in Init, \quad \forall t \geq 0 \qquad p(\Phi(x^*, t)) = 0$$

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{v_x} \\ \dot{v_y} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1/2 \\ 0 & 0 & 1/2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ v_x \\ v_y \end{pmatrix}$$

$v_x^* = 2, v_y^* = -2 \implies v_x^2 + v_y^2 = 8$ (conservation of energy)

Linear Systems
Solution

1. **Solving the system** of differential equations
   - Linear systems can be explicitly solved

2. **Eliminating** the terms involving **time**
   - Adding auxiliary variables to handle non-algebraic terms (exponentials, trigonometric terms)
   - Adding auxiliary equations relating the auxiliary variables

Linear Systems
Solving the System

- Solution to $\dot{x} = Ax + B$ with initial condition x^*

$$\Phi(x^*, t) = e^{At}x^* + e^{At}(\int_0^t e^{-A\tau}d\tau)\ B$$

- It can be expressed as **polynomials** in t, $e^{\pm at}$, $\cos(bt)$, $\sin(bt)$, where $\lambda = a + bi$ are **eigenvalues** of matrix A.

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{v_x} \\ \dot{v_y} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1/2 \\ 0 & 0 & 1/2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ v_x \\ v_y \end{pmatrix}$$

$$\begin{cases} x &= x^* + 2\sin(t/2)\, v_x^* + (2\cos(t/2) - 2)\, v_y^* \\ y &= y^* + (-2\cos(t/2) + 2)\, v_x^* + 2\sin(t/2)\, v_y^* \\ v_x &= \cos(t/2)\, v_x^* - \sin(t/2)\, v_y^* \\ v_y &= \sin(t/2)\, v_x^* + \cos(t/2)\, v_y^* \end{cases}$$

Linear Systems
Eliminating Time (1)

- **Simple case:**
  eigenvalues of matrix A have real and imaginary parts in $\mathbb{Q}$
  Then:

  - $\exists p \in \mathbb{Q}$ such that for all exponential terms e^{at}:

    $$e^{at} = (e^{pt})^c \text{ for a certain } c \in \mathbb{Z}$$

    If we introduce new variables $u = e^{pt}$, $v = e^{-pt}$,
    then either $e^{at} = u^{|c|}$ or $e^{at} = v^{|c|}$

  - For trigonometric terms, similarly for a certain $q \in \mathbb{Q}$ and new variables $w = \cos(qt)$, $z = \sin(qt)$

Linear Systems
Eliminating Time (2)

$$\left\{\begin{array}{rcl} x & = & x^* + 2\sin(t/2)\, v_x^* + (2\cos(t/2) - 2)\, v_y^* \\ y & = & y^* + (-2\cos(t/2) + 2)\, v_x^* + 2\sin(t/2)\, v_y^* \\ v_x & = & \cos(t/2)\, v_x^* - \sin(t/2)\, v_y^* \\ v_y & = & \sin(t/2)\, v_x^* + \cos(t/2)\, v_y^* \end{array}\right.$$

$$\Downarrow$$

$$w = \cos(t/2), z = \sin(t/2)$$

$$\Downarrow$$

$$\left\{\begin{array}{rcl} x & = & x^* + 2zv_x^* + (2w - 2)v_y^* \\ y & = & y^* + (-2w + 2)\, v_x^* + 2zv_y^* \\ v_x & = & wv_x^* - zv_y^* \\ v_y & = & zv_x^* + wv_y^* \end{array}\right.$$

Linear Systems
Eliminating Time (3)

- **Eliminate auxiliary variables** using
  - auxiliary equations $uv = 1$, $w^2 + z^2 = 1$
  - Gröbner bases with an elimination term ordering where the auxiliary variables are the biggest ones

INITIAL CONDITIONS

$$\begin{cases} v_x^* &= 2 \\ v_y^* &= -2 \end{cases}$$

FLOW

$$\begin{cases} x &= x^* + 2zv_x^* + (2w-2)v_y^* \\ y &= y^* + (-2w+2)\, v_x^* + 2zv_y^* \\ v_x &= wv_x^* - zv_y^* \\ v_y &= zv_x^* + wv_y^* \end{cases}$$

AUXILIARY EQUATIONS

$$\left\{ w^2 + z^2 = 1 \right.$$

$$\Downarrow$$

$$v_x^2 + v_y^2 = 8$$

Linear Systems
Eliminating Time (4)

- **General case:** similarly by computing $\mathbb{Q}$-bases of the real and imaginary parts of the eigenvalues of the matrix A
  - Exponential terms: new variables x_1, y_1, ..., x_k, y_k satisfying $x_i y_i = 1$
  - Trigonometric terms: new variables w_1, z_1, ..., w_l, z_l satisfying $w_j^2 + z_j^2 = 1$
- **MAIN RESULT:**
  all polynomial invariants of the system are generated

Overview of the Talk

1. **Finding Invariants for Linear Systems**
2. **Abstract Interpretation**
3. **Finding Invariants for Hybrid Systems**
4. **Related Work**
5. **Future Work & Conclusions**

Abstract Interpretation (1)

Abstract interpretation is a framework for computing invariants of several kinds:

- intervals (Cousot & Cousot 1976, Harrison 1977)

$$x \in [0, 1] \ \wedge \ y \in [0, \infty)$$

- linear inequalities (Cousot & Halbwachs 1978, Colón & Sankaranarayanan & Sipma 2003)

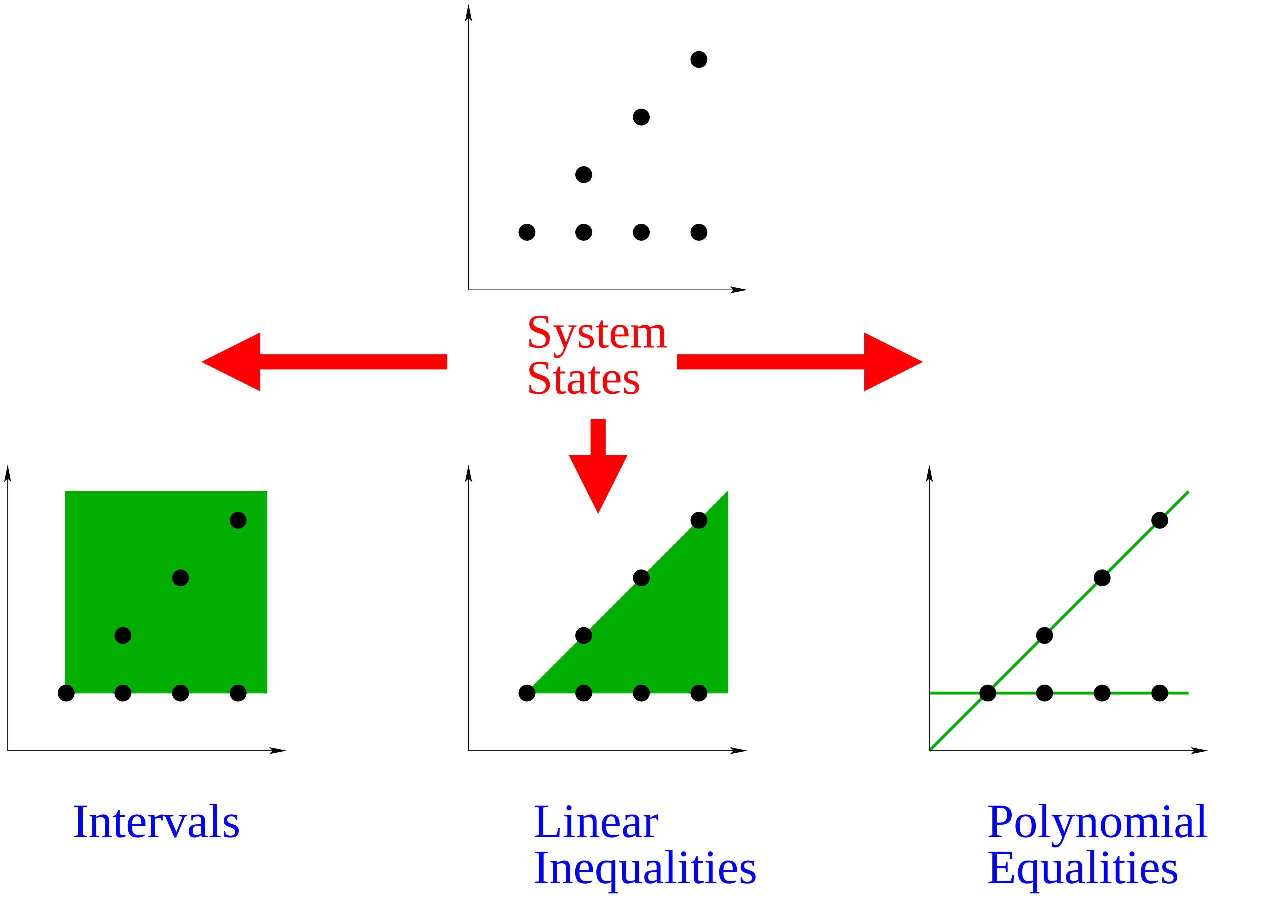
$$x + 2y - 3z \leq 3$$

- ...
- **polynomial equalities** (Müller-Olm & Seidl 2004, Sankaranarayanan & Sipma& Manna 2004, Colón 2004, Rodríguez-Carbonell & Kapur 2004)

$$x = y^2$$

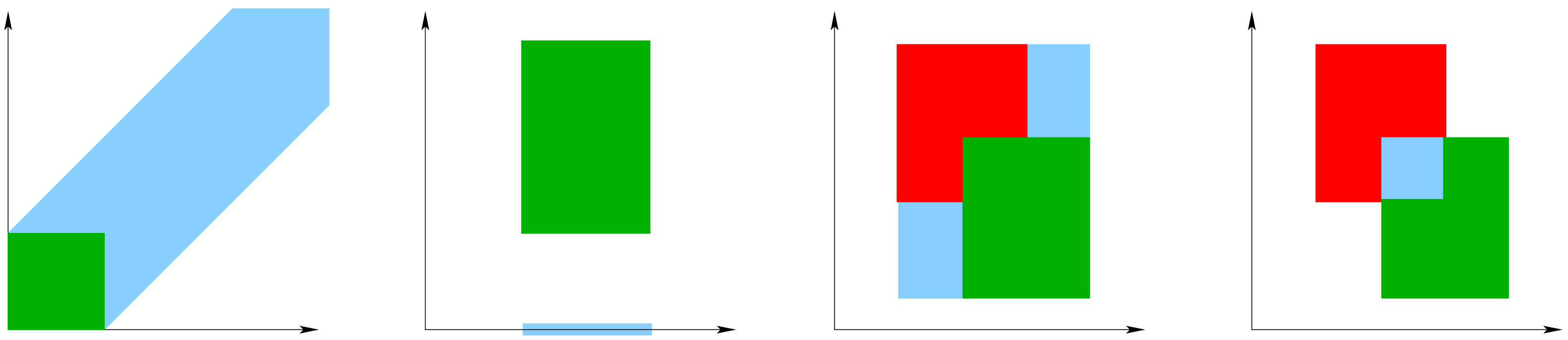
Abstract Interpretation (2)

Concrete variable values overapproximated by *abstract values*



Abstract Interpretation (3)

- Semantics of hybrid systems in terms of abstract values
- Operations on concrete states must be abstracted:



Time Elapse   Image   Union   Intersection

- Invariants are generated by the symbolic execution of the hybrid system using the abstract semantics

Overview of the Talk

1. **Finding Invariants for Linear Systems**
2. **Abstract Interpretation**
3. **Finding Invariants for Hybrid Systems**
4. **Related Work**
5. **Future Work & Conclusions**

Hybrid Systems
Ideals of Polynomials

- Intuitively, an **ideal** is a set of polynomials and their consequences

- An **ideal** is a set of polynomials I such that
  1. $0 \in I$
  2. If $p, q \in I$, then $p + q \in I$
  3. If $p \in I$ and q any polynomial, $pq \in I$

- Example: multiples of a polynomial p, $\langle p \rangle$
  1. $0 = 0 \cdot p \in \langle p \rangle$
  2. $q_1 \cdot p + q_2 \cdot p = (q_1 + q_2)p \in \langle p \rangle$
  3. If q_2 is any polynomial, then $q_2 \cdot q_1 \cdot p \in \langle p \rangle$

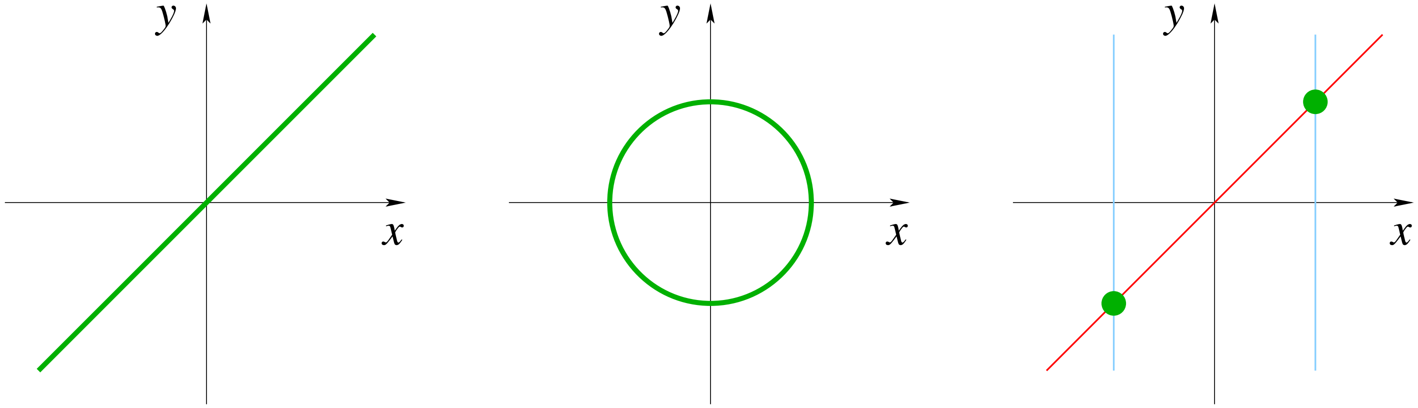
- In general, ideal generated by $p_1, \ldots, p_k$:

$$\langle p_1, \ldots, p_k \rangle = \{\sum_{j=1}^{k} q_j \cdot p_j \text{ for arbitrary } q_j\}$$

Hybrid Systems

Ideals as Abstract Values

$$\langle p_1, \ldots, p_k \rangle \longleftrightarrow p_1 = 0 \wedge \cdots \wedge p_k = 0$$



$x = y$	$x^2 + y^2 = 1$	$\boxed{x^2 = x} \wedge \boxed{x = y}$
$\Updownarrow$	$\Updownarrow$	$\Updownarrow$
$\langle x - y \rangle$	$\langle x^2 + y^2 - 1 \rangle$	$\langle x^2 - x, x - y \rangle$

Hybrid Systems

Abstract Semantics

- time elapse $\longrightarrow$ solve differential equations, eliminate time
- image of states $\longrightarrow$ projection of ideals:

$$I \cap \mathbb{C}[x_1, ..., x_{i-1}, x_{i+1}, ..., x_n]$$

- union of states $\longrightarrow$ intersection of ideals:

$$I \cap J$$

- intersection with equality guards $\longrightarrow$ addition of ideals:

$$I + J = \{p + q \mid p \in I, q \in J\}$$

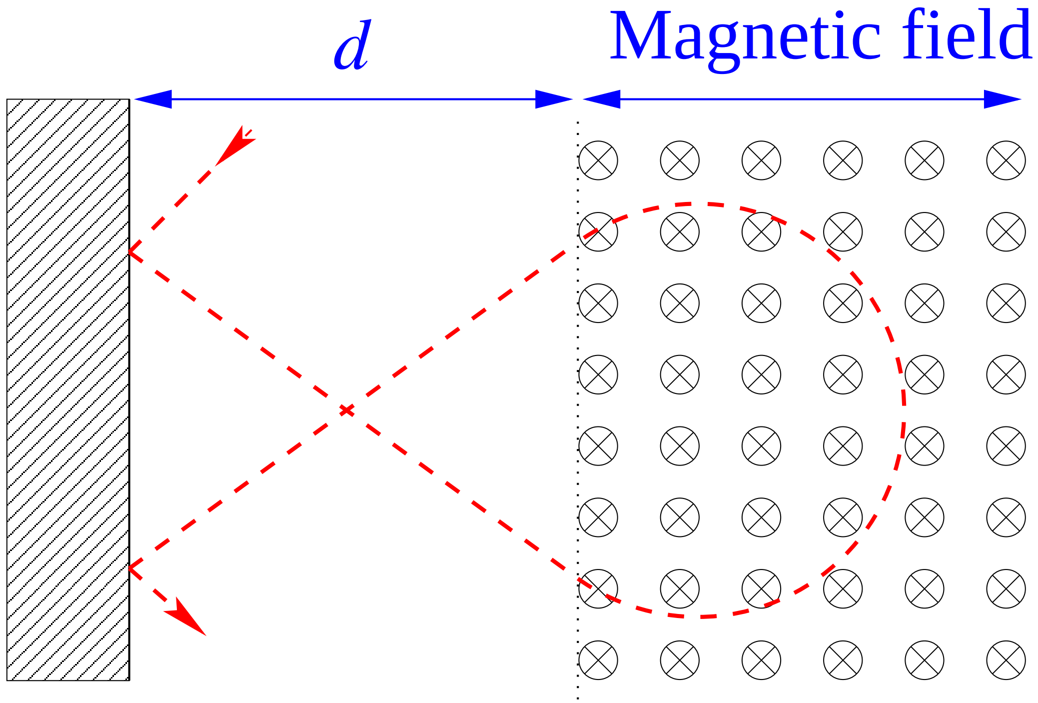
- intersection with disequality guards $\longrightarrow$ quotient of ideals:

$$I : J = \{p \mid \forall q \in J, p \cdot q \in I\}$$

All operations can be implemented using **Gröbner bases**

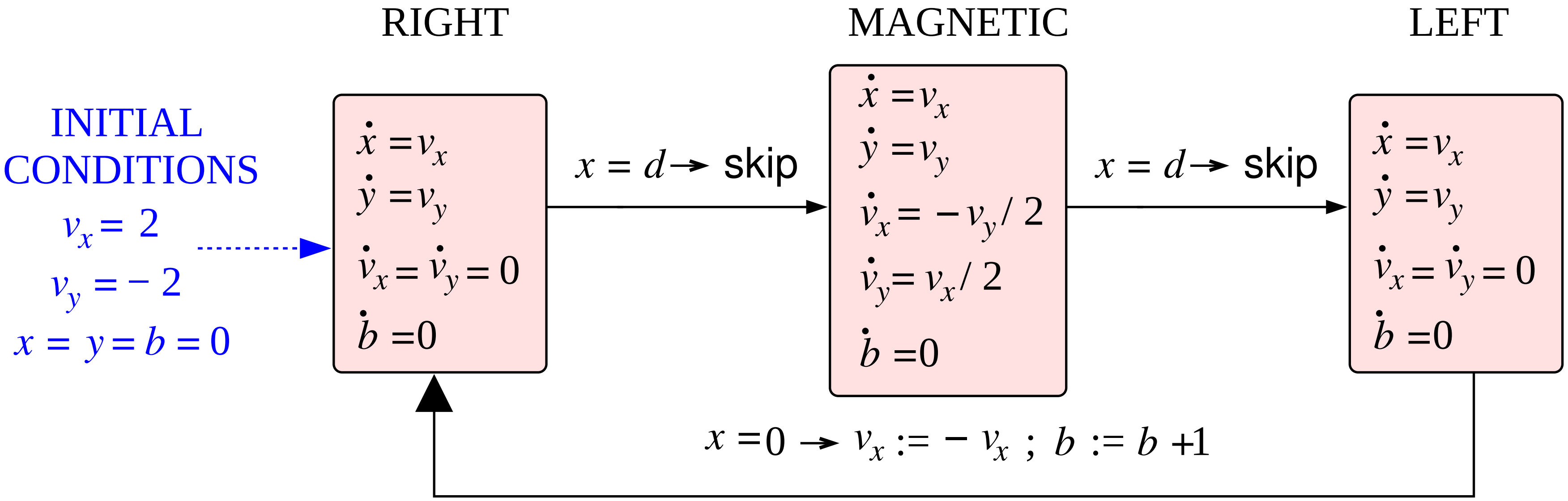
Hybrid Systems

Example (1)



Hybrid Systems
Example (2)

Variable b counts the number of bounces against the wall



RIGHT $\rightarrow$ $v_y = -2 \wedge v_x = 2 \wedge 2db - 8b + y + x = 0$

MAGNETIC $\rightarrow$ $x - 2v_y - d = 4 \wedge v_x^2 + v_y^2 = 8 \wedge 2v_x + y + 2db - 8b + d = 4$

LEFT $\rightarrow$ $v_y = -2 \wedge v_x = -2 \wedge 2db - 8b + y - x = 8$

Overview of the Talk

1. **Finding Invariants for Linear Systems**
2. **Abstract Interpretation**
3. **Finding Invariants for Hybrid Systems**
4. **Related Work**
5. **Future Work & Conclusions**

Related Work (1)

- (Sankaranarayanan & Sipma & Manna, 2004):
  discovery of polynomial equality invariants using
  constrained-based invariant generation and heuristics

- Advantages:
  - Polynomial vector fields allowed in differential equations

- Disadvantages:
  - No completeness result

Related Work (2)

- (Laferriere & Pappas & Yovine, 1999):
  computation of the **exact** reachability set using polynomial inequalities and quantifier elimination
- Advantages:
  - Polynomial inequalities more expressive than equalities: exact characterization of the reachability set
- Disadvantages:
  - More restricted linear systems: eigenvalues in $\mathbb{Q}$ or $i \cdot \mathbb{Q}$
  - Quantifier elimination more costly than Gröbner bases

Overview of the Talk

1. **Finding Invariants for Linear Systems**
2. **Abstract Interpretation**
3. **Finding Invariants for Hybrid Systems**
4. **Related Work**
5. **Future Work & Conclusions**

Future Work

- Handle more general classes of systems of differential equations

- Extend the method to generate polynomial inequalities as invariants

- Apply the resulting method to improve linear inequality invariants

Conclusions

- Method for finding **all** polynomial equality invariants of linear systems:

  1. Solve differential equations
  2. Eliminate time with Gröbner bases

     - Auxiliary variables

$$\begin{array}{rclcrcl} u_i & \leftrightarrow & e^{pt} & \qquad & w_i & \leftrightarrow & \cos(qt) \\ v_i & \leftrightarrow & e^{-pt} & & z_i & \leftrightarrow & \sin(qt) \end{array}$$

     - Auxiliary equations:

$$u_i v_i = 1, \qquad w_i^2 + z_i^2 = 1$$

- Extension to hybrid systems using the abstract interpretation framework