An Algorithmic Approach to Global Asymptotic Stability Verification of Hybrid Systems

Miriam García Soto & Pavithra Prabhakar
IMDEA Software Institute & Kansas State University

EMSOFT'16

Pittsburgh, PA, USA

Hybrid Systems

Cyber-Physical Systems

Systems controlled by computer-based algorithms integrated in the physical world.

Medical Devices

Automotive

Robotics

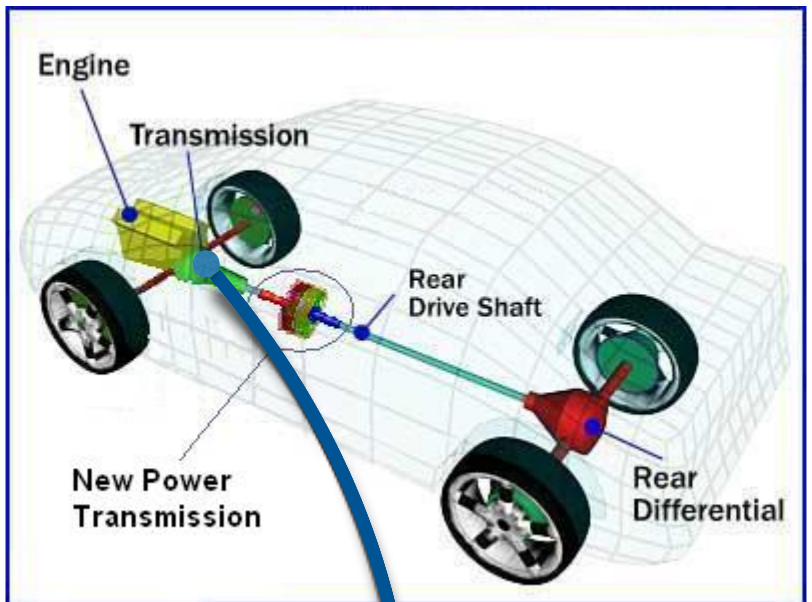
Process control

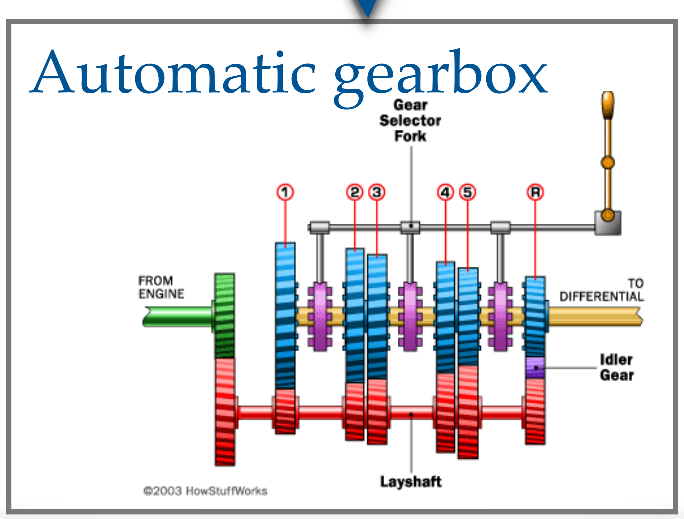
- Combine control, communication and computation.
- Design methodology for building high-confidence systems.
- Discrete and continuous behaviour.

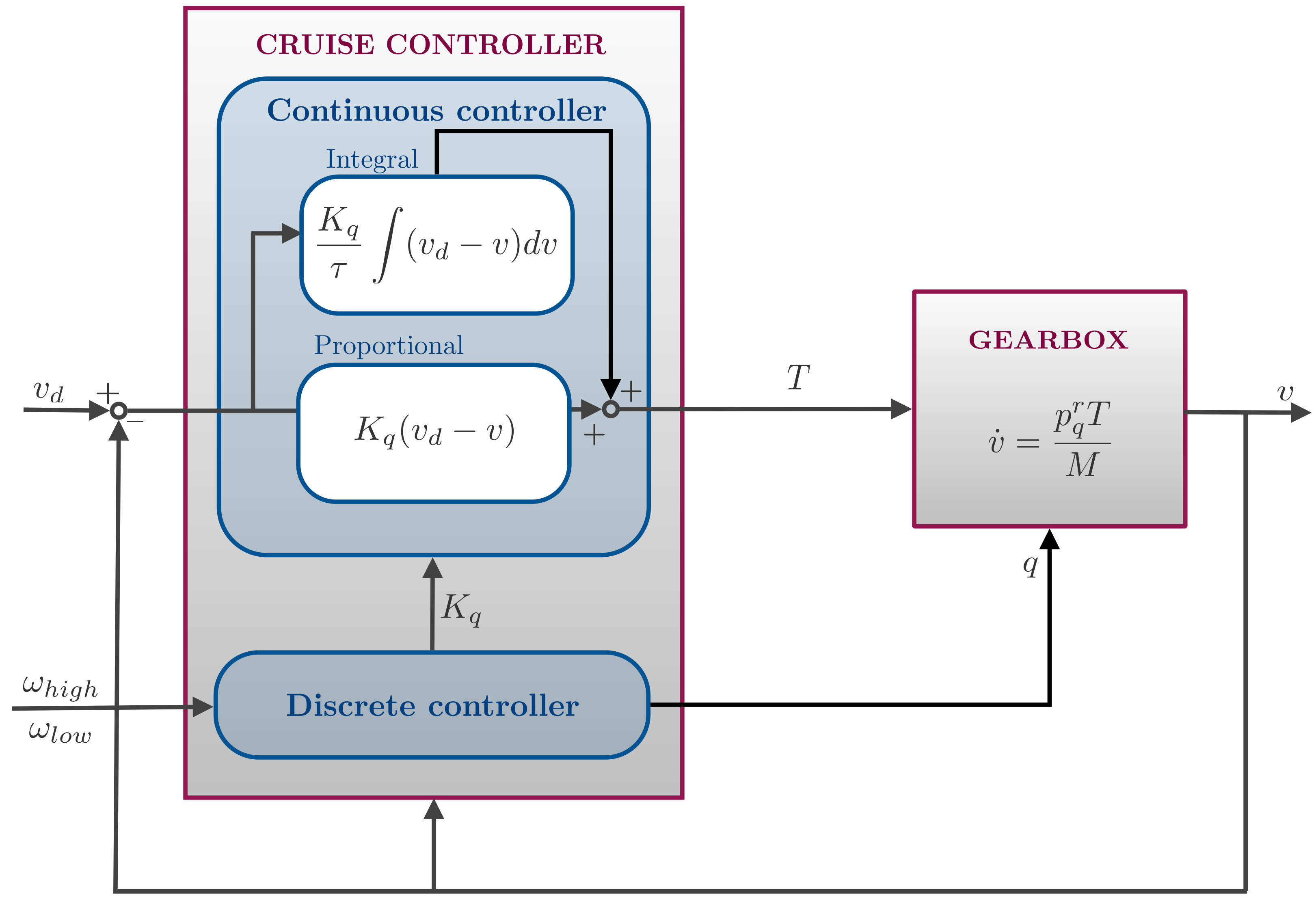
Hybrid System

System exhibiting a mixed **continuous** and **discrete** behaviour.

Cruise control and automatic gearbox

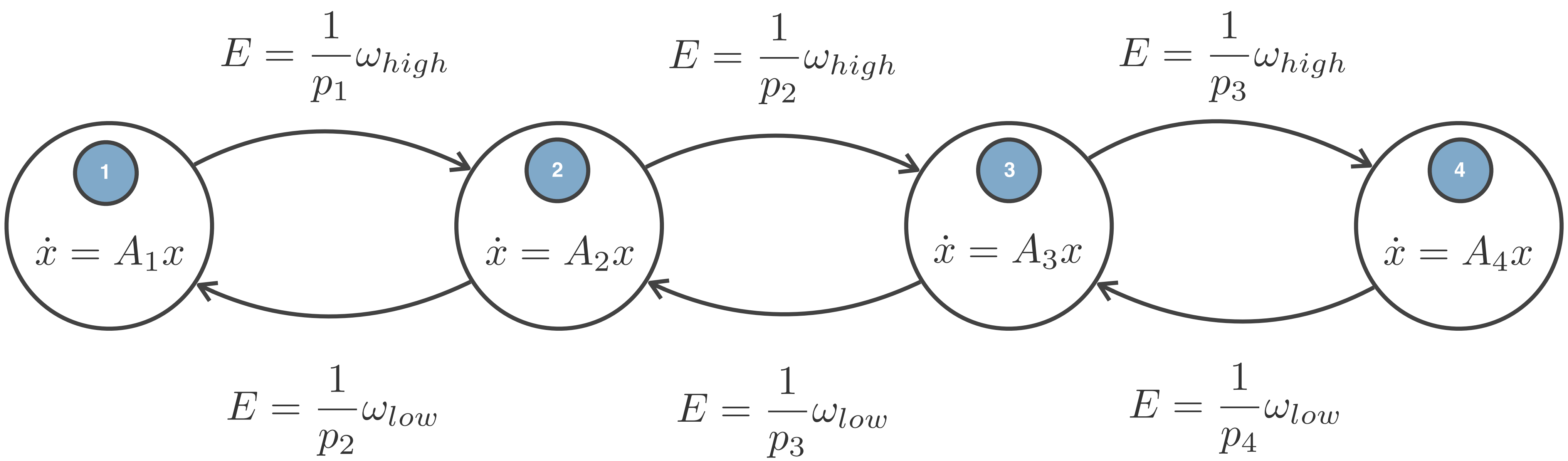






Drive the vehicle velocity to a desired velocity.

Automatic gearbox: a hybrid system



Dynamical equations

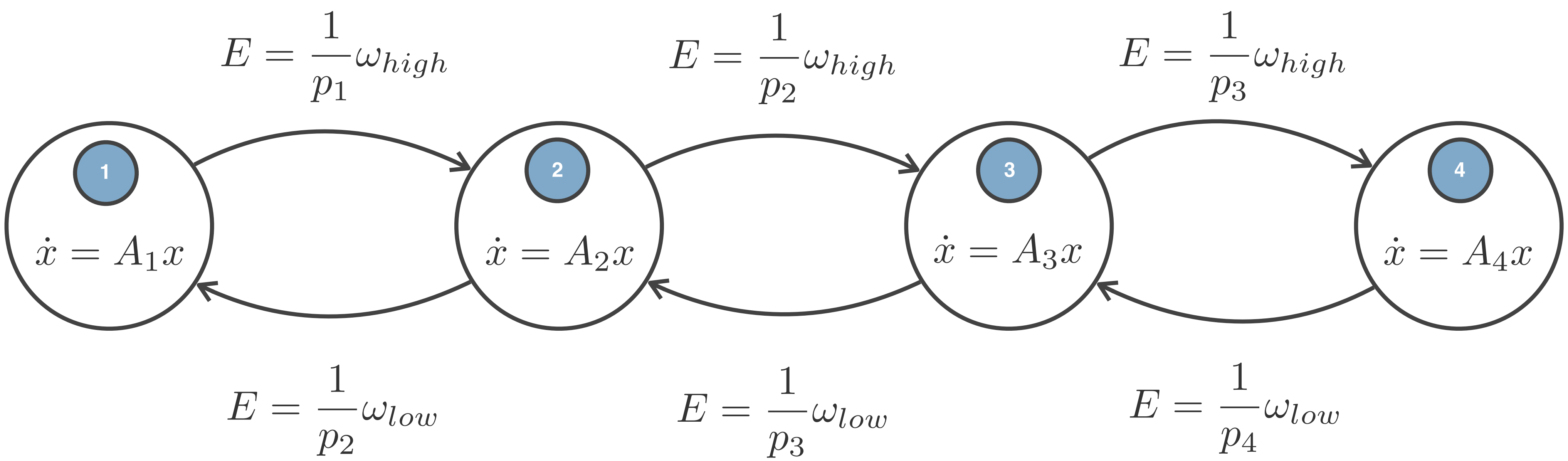
$$\dot{E} = -\frac{p_q}{Mr} K_q E - \frac{p_q}{Mr} T_I$$

$$\dot{T}_I = -\frac{K_q}{\tau} E$$

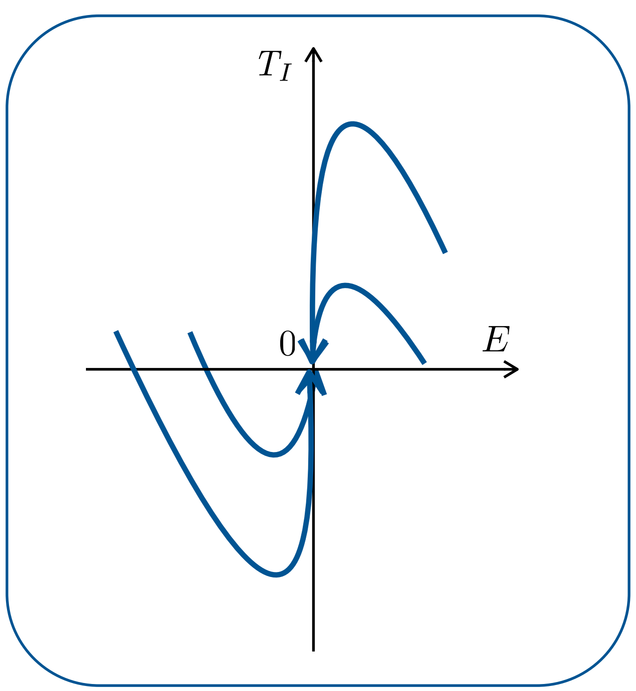
$$x = \begin{pmatrix} E \\ T_I \end{pmatrix}$$

$E = v_d - v$	Difference between desired and current velocity
T_I	Integral part of the torque

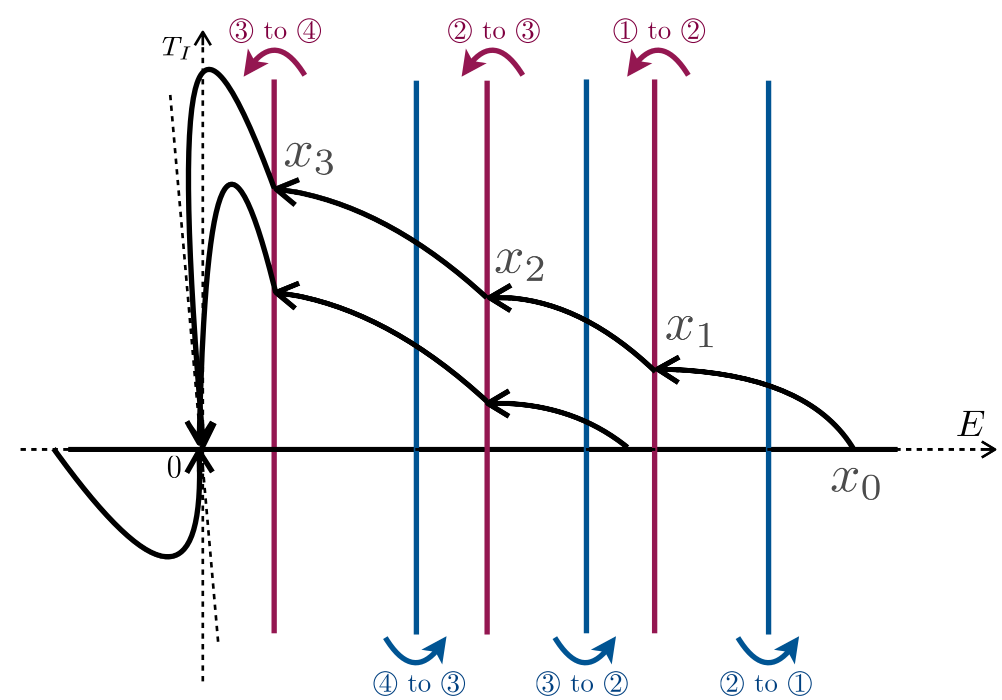
Automatic gearbox: a hybrid system



Dynamics



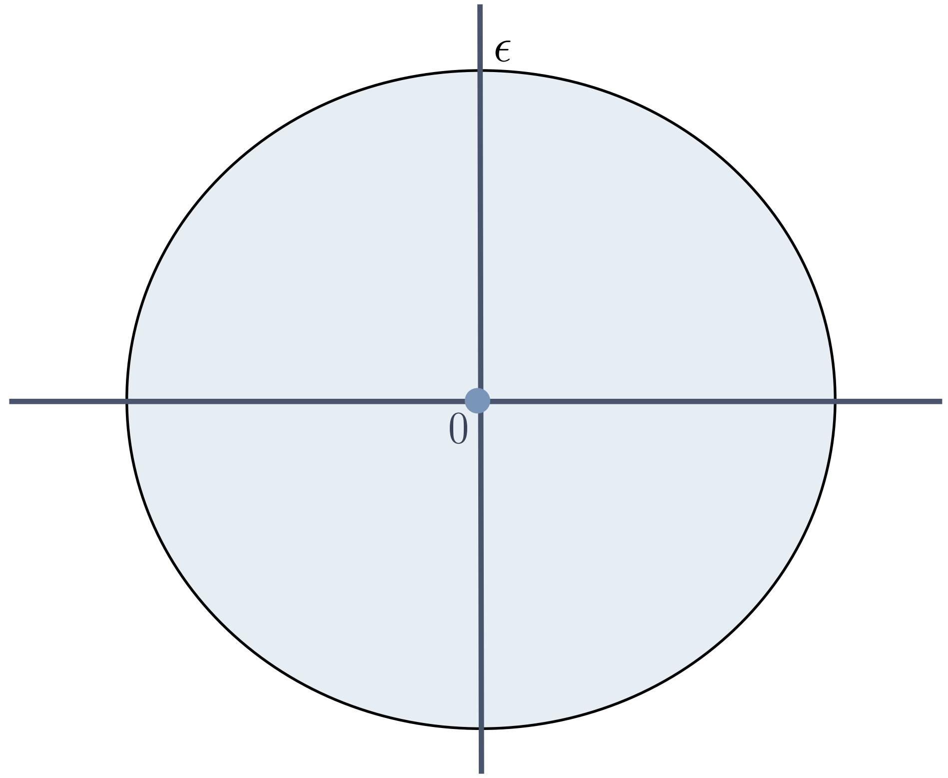
Executions



Stability Notions

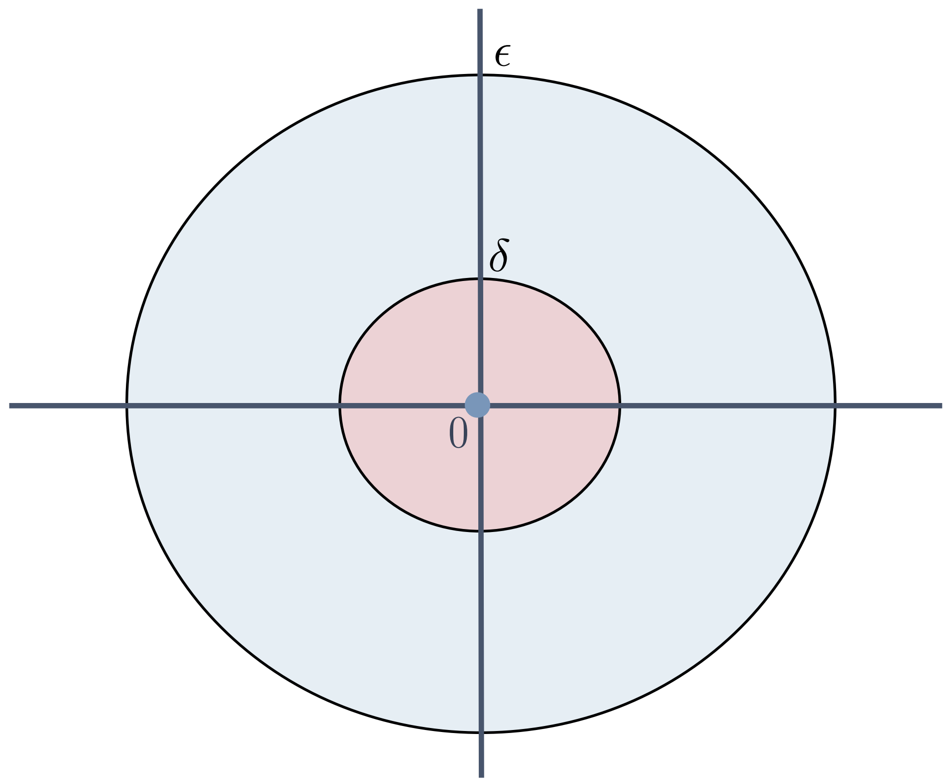
Lyapunov Stability (LS)

A system is Lyapunov stable with respect to 0 if for every $\varepsilon > 0$ there exists $\delta > 0$ such that every execution σ starting from $B_\delta(0)$ implies $\sigma \in B_\varepsilon(0)$.



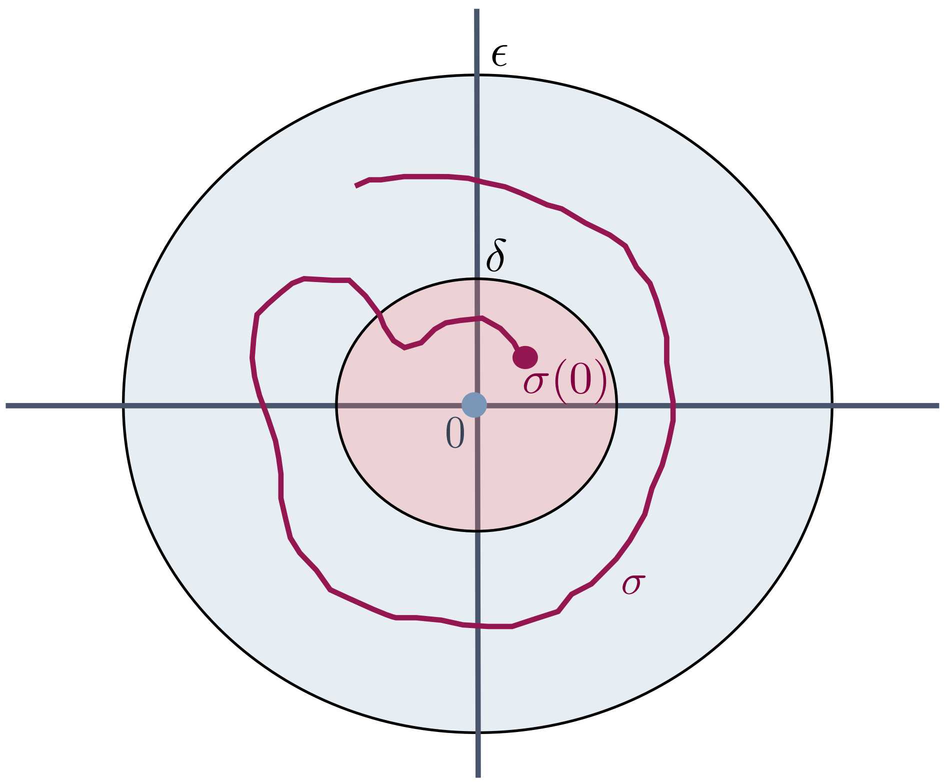
Lyapunov Stability (LS)

A system is Lyapunov stable with respect to 0 if for every $\varepsilon > 0$ there exists $\delta > 0$ such that every execution σ starting from $B_\delta(0)$ implies $\sigma \in B_\varepsilon(0)$.



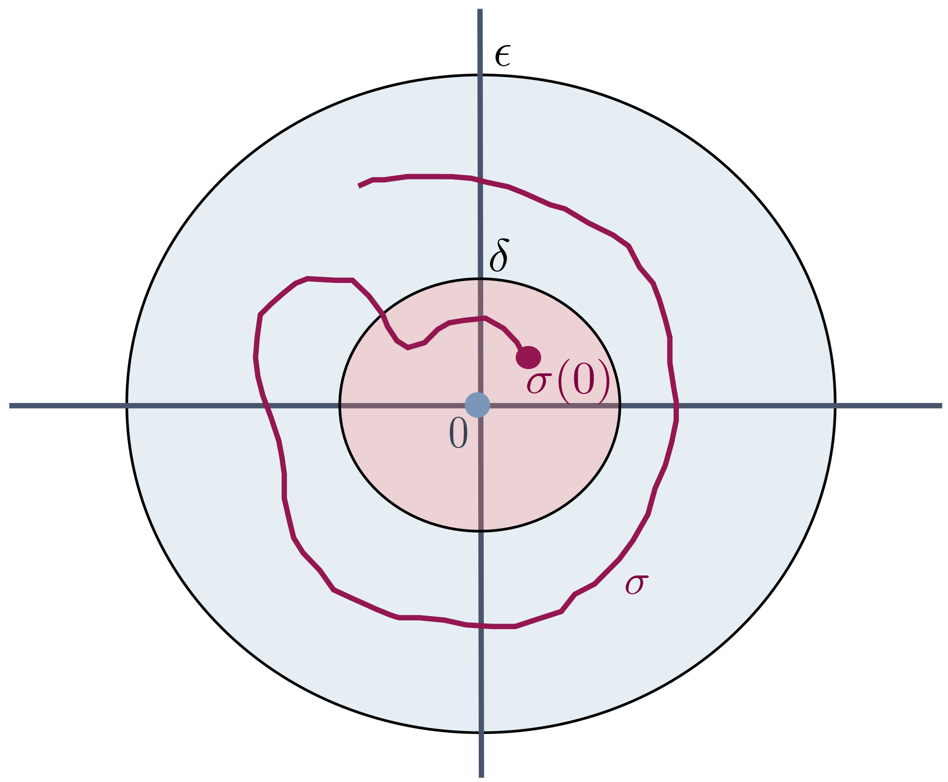
Lyapunov Stability (LS)

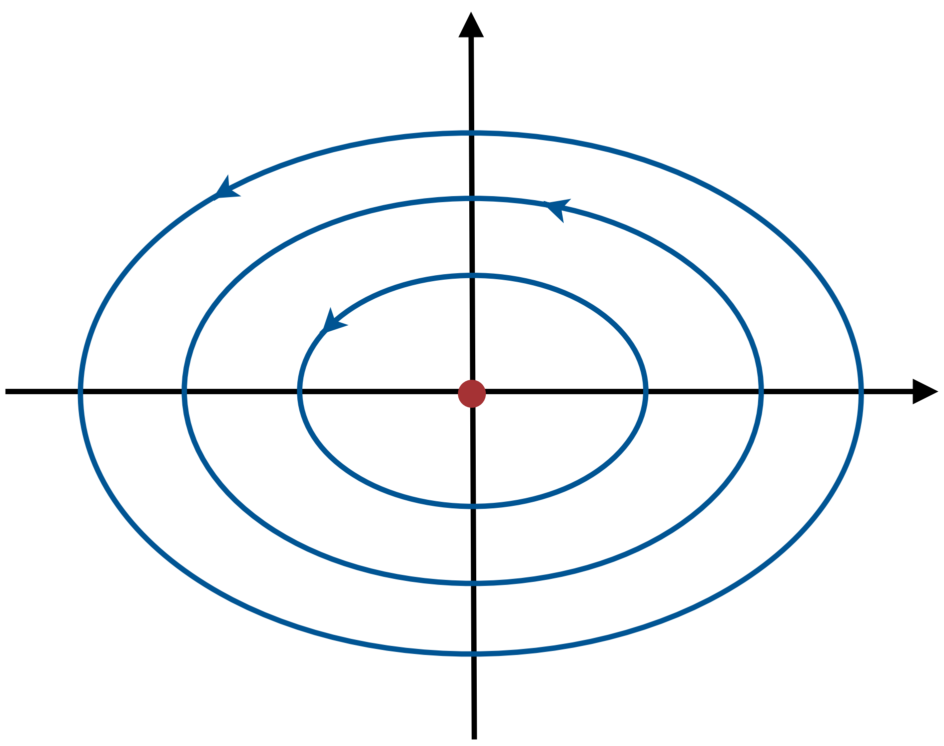
A system is Lyapunov stable with respect to 0 if for every $\varepsilon > 0$ there exists $\delta > 0$ such that every execution σ starting from $B_\delta(0)$ implies $\sigma \in B_\varepsilon(0)$.



Lyapunov Stability (LS)

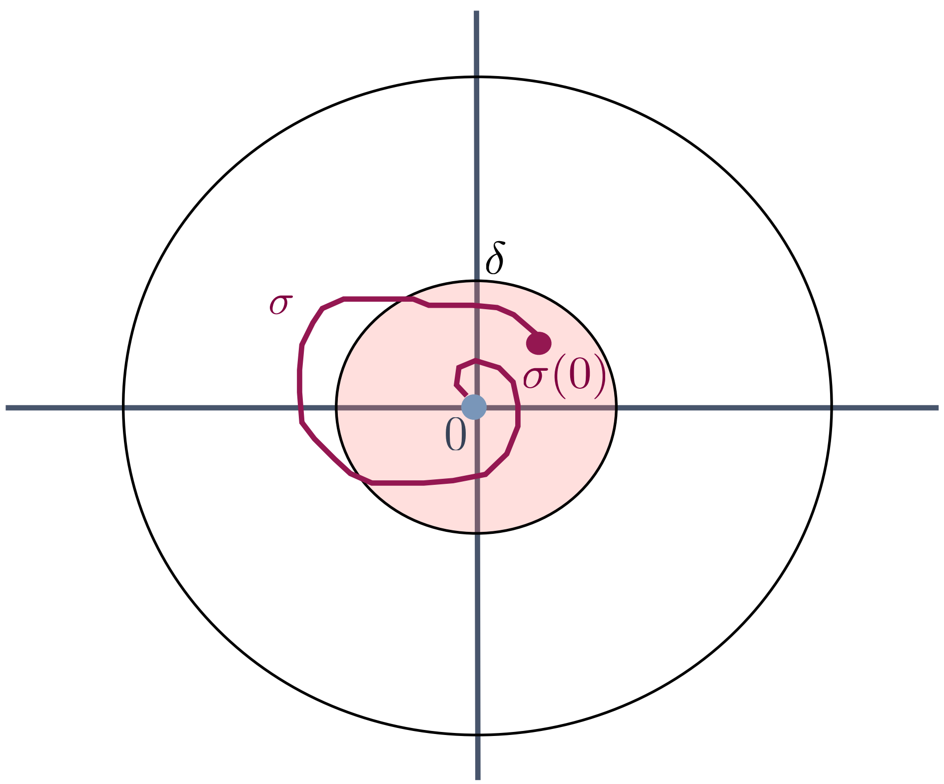
A system is Lyapunov stable with respect to 0 if for every $\varepsilon > 0$ there exists $\delta > 0$ such that every execution σ starting from $B_\delta(0)$ implies $\sigma \in B_\varepsilon(0)$.

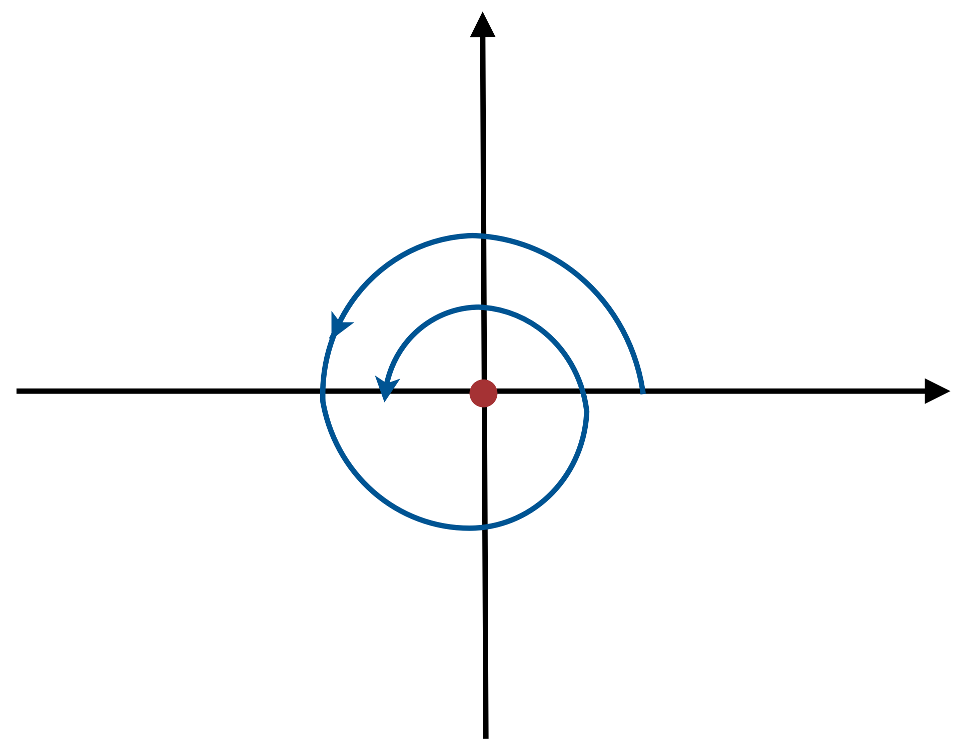




Asymptotic Stability (AS)

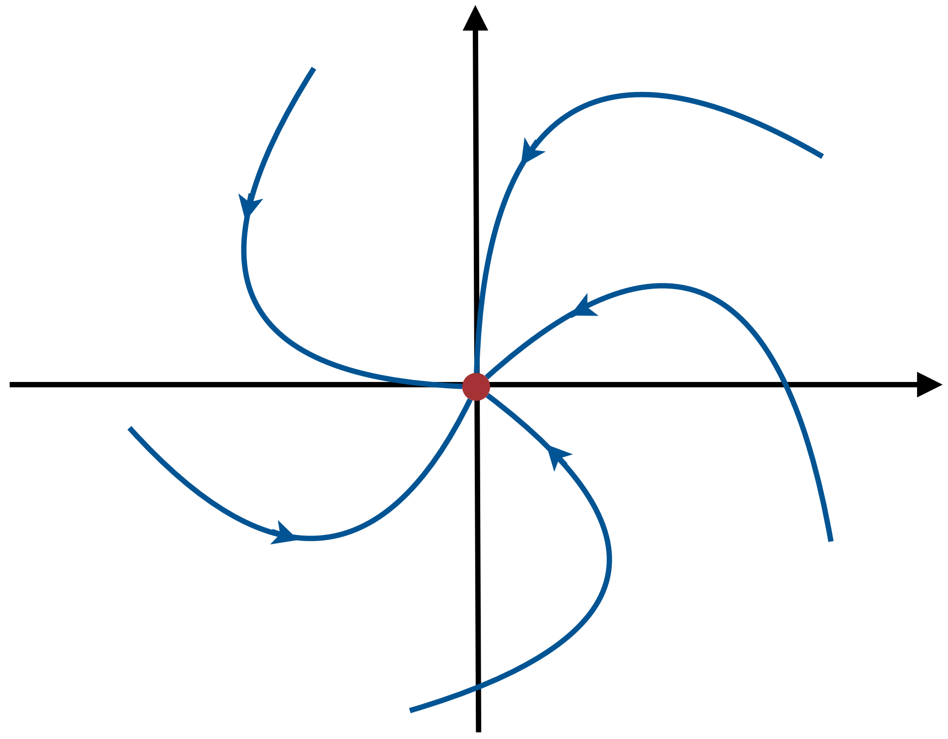
A system is AS with respect to 0 if it is Lyapunov stable and there exists a value $\delta > 0$ such that every execution σ starting from $B_\delta(0)$ converges to 0.



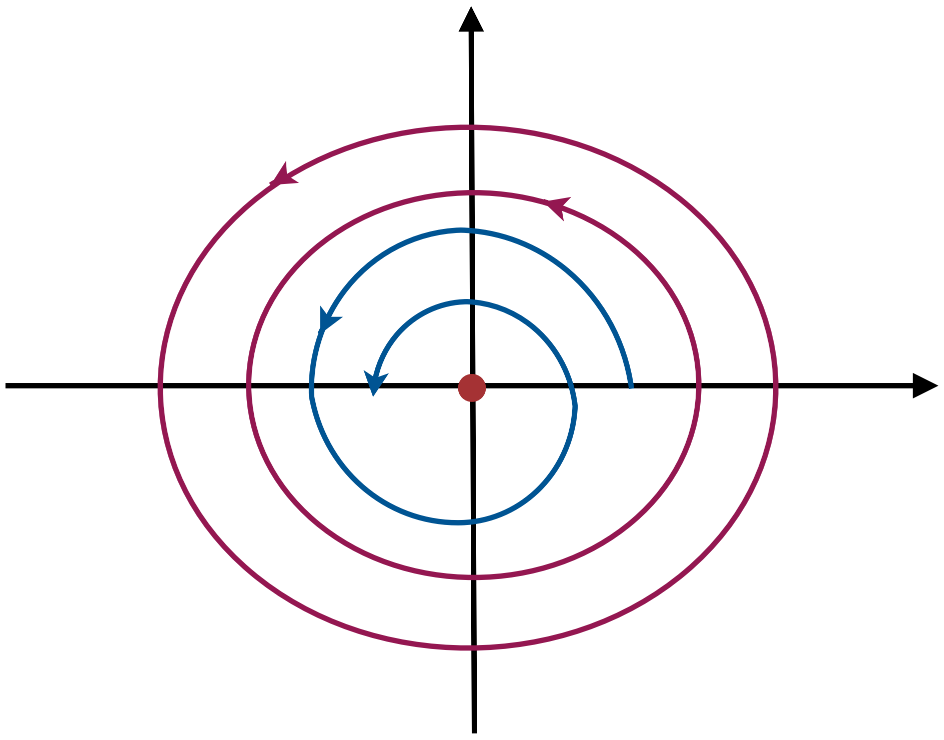


Global Asymptotic Stability (GAS)

A system is GAS with respect to 0 if it is Lyapunov stable and every execution σ converges to 0.



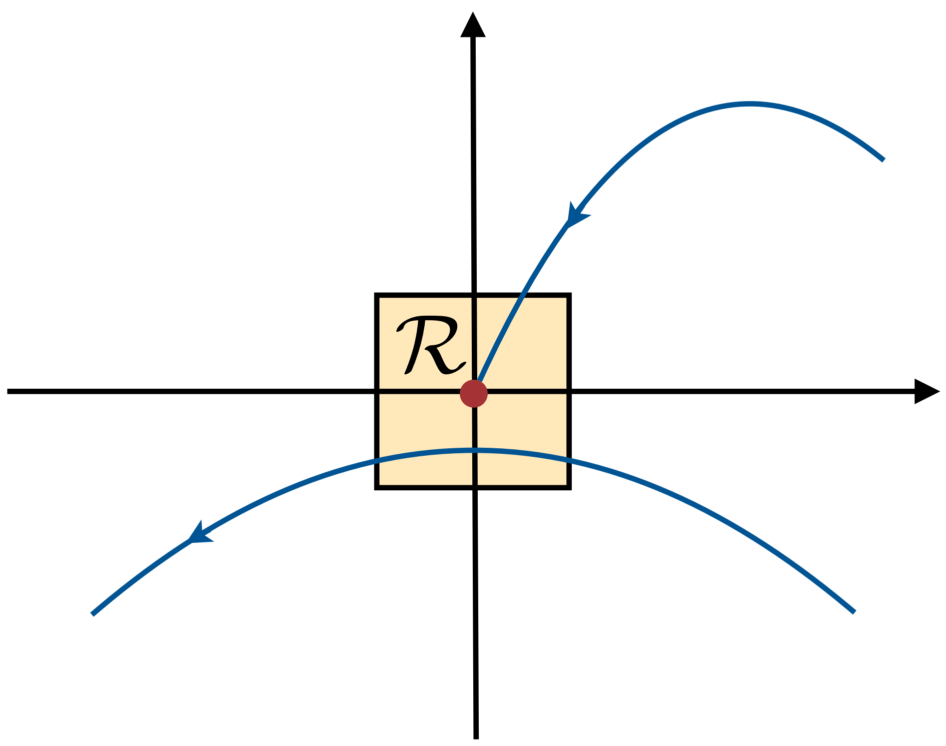
Global asymptotic stability



Asymptotic stability

Region Stability (RS)

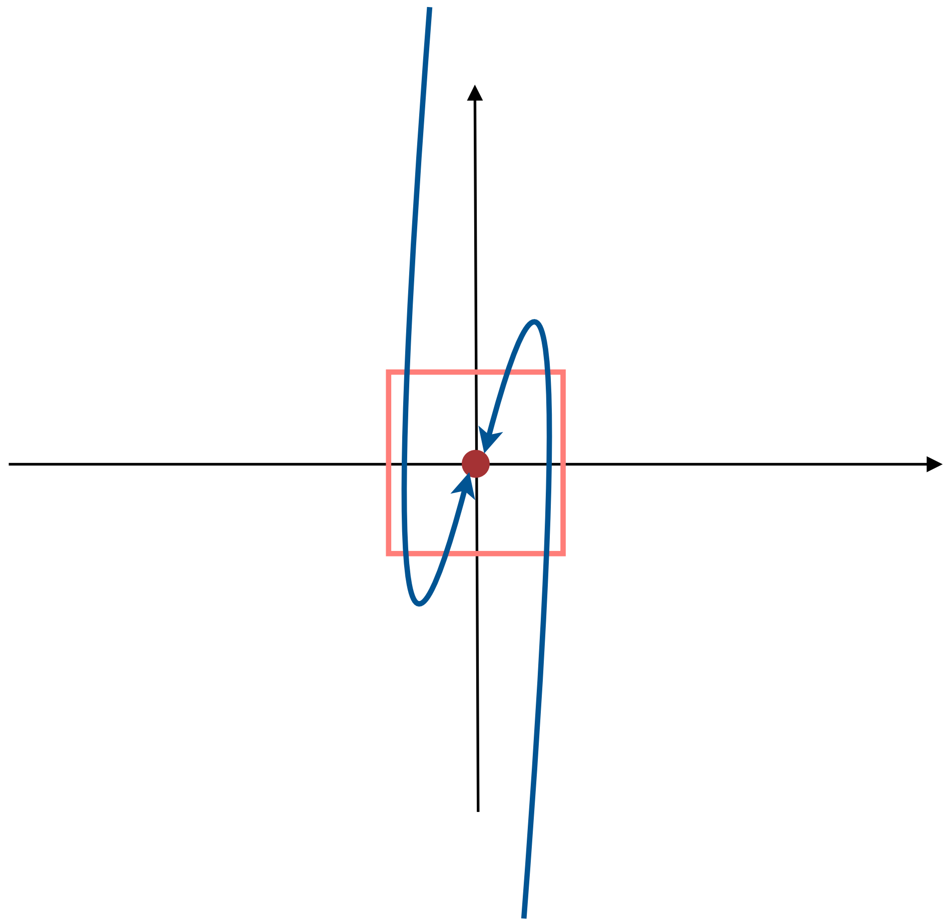
A system is RS with respect to R if for every execution σ there exists a value T ≥ 0 such that σ at time T belongs to R.

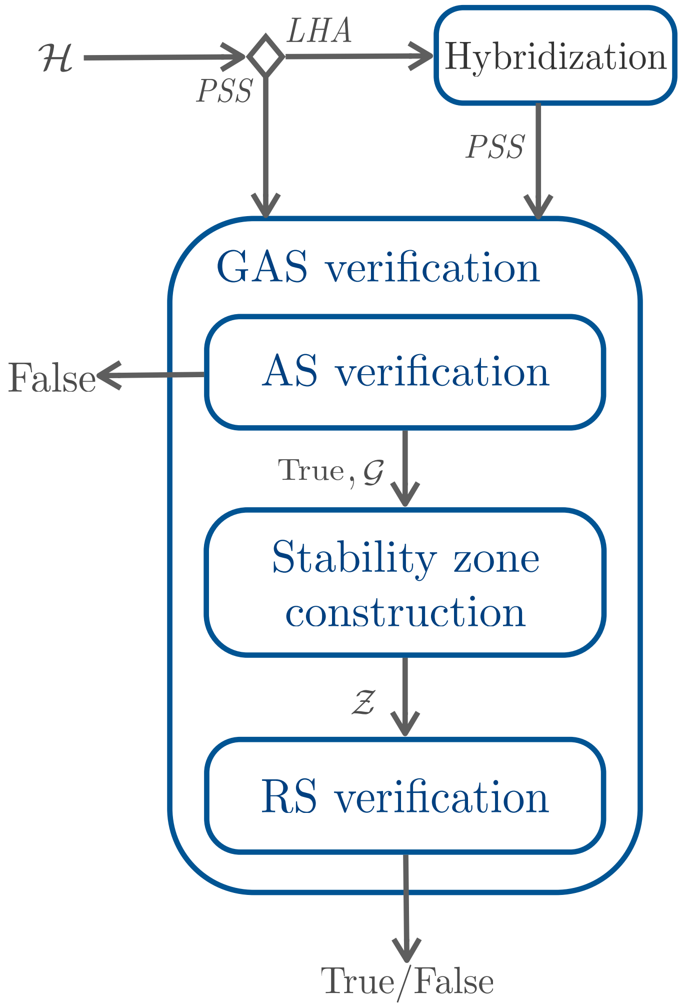


Global Asymptotic Stability Verification

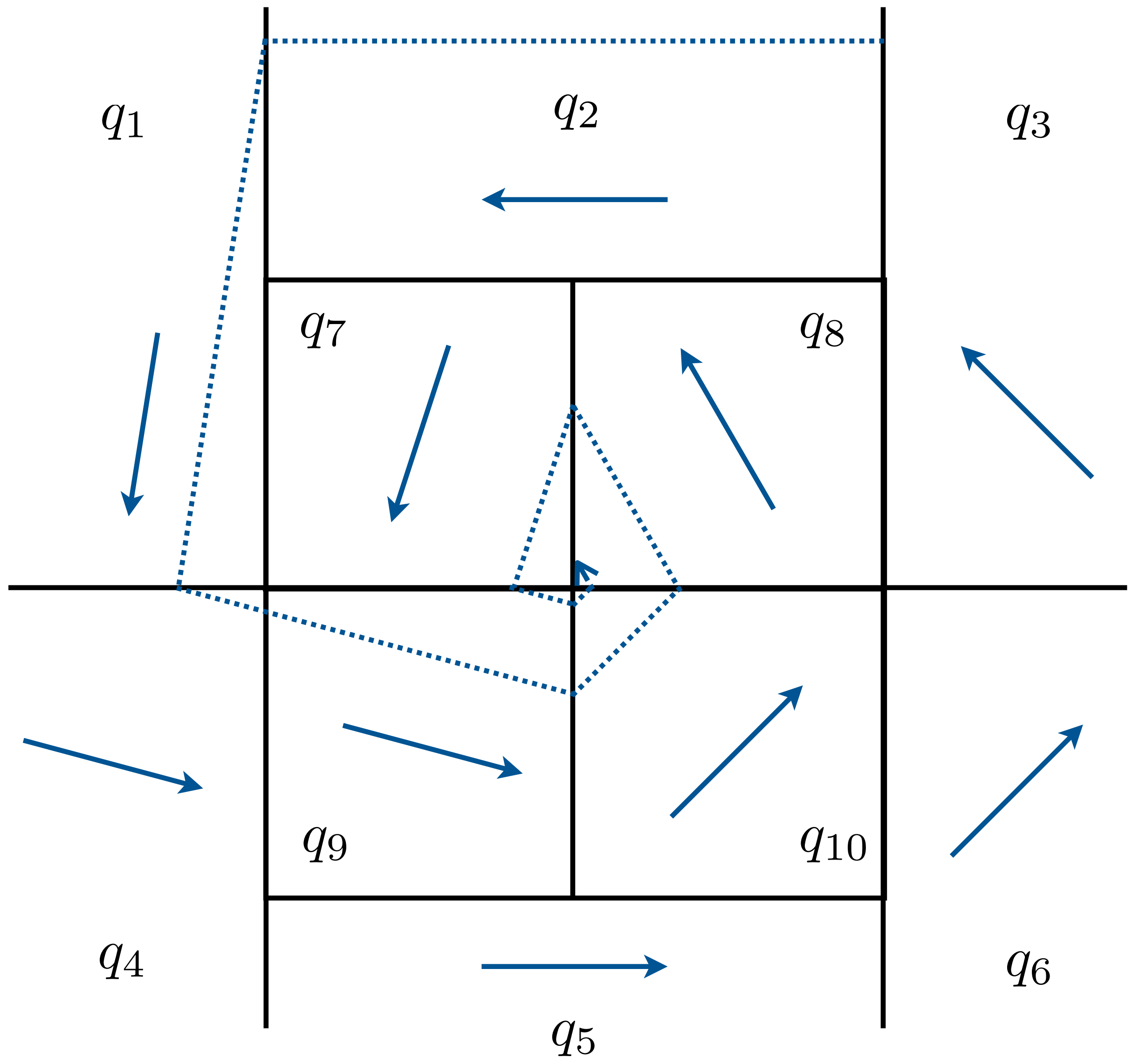
GAS verification

- **Step 1 :** Asymptotic Stability (AS) verification
- **Step 2 :** Stability zone construction
- **Step 3 :** Region Stability (RS) verification



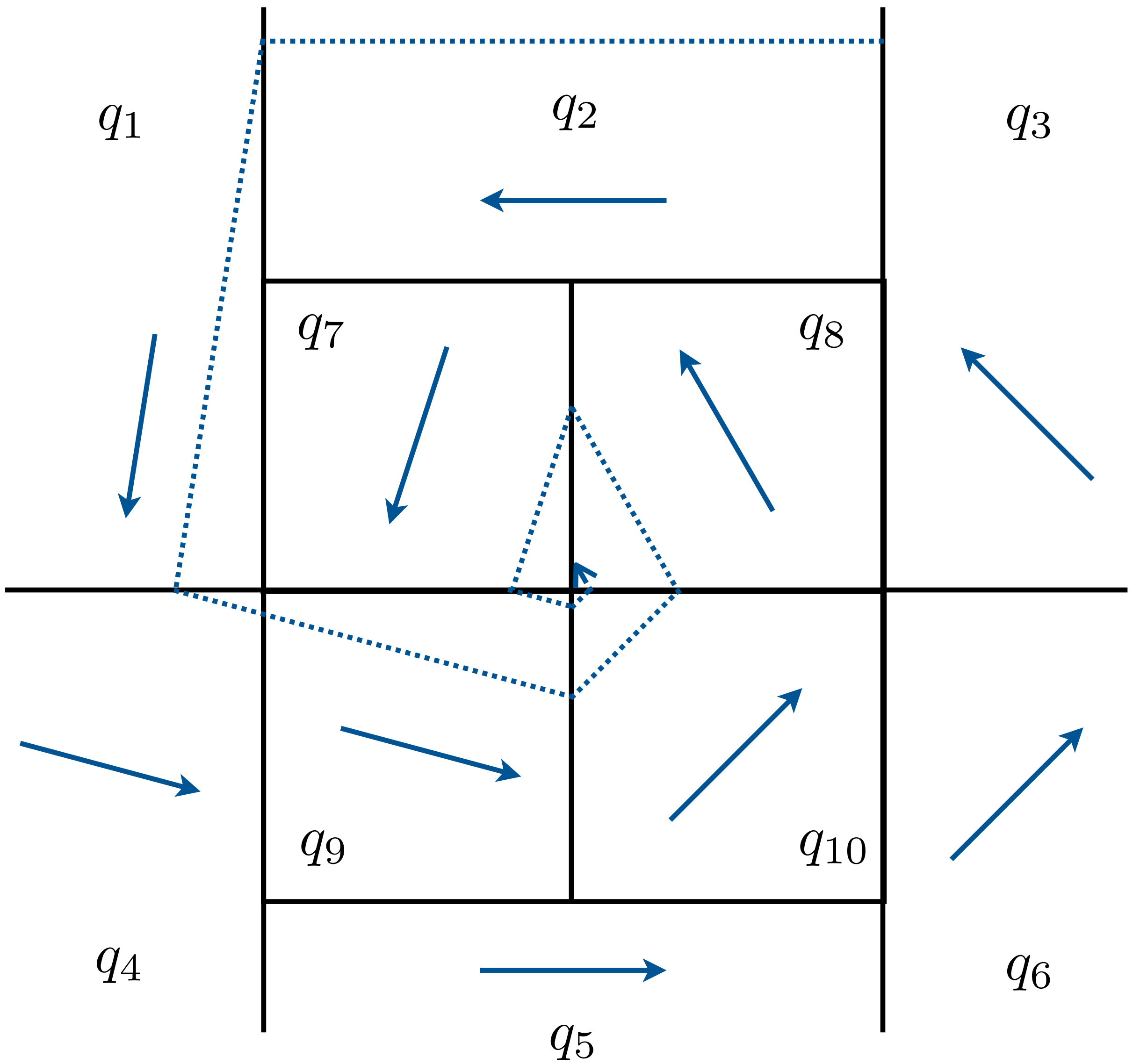


Polyhedral Switched System (PSS)



- Dynamics are modelled by polyhedral inclusions.
- Invariants and guards are polyhedral sets.

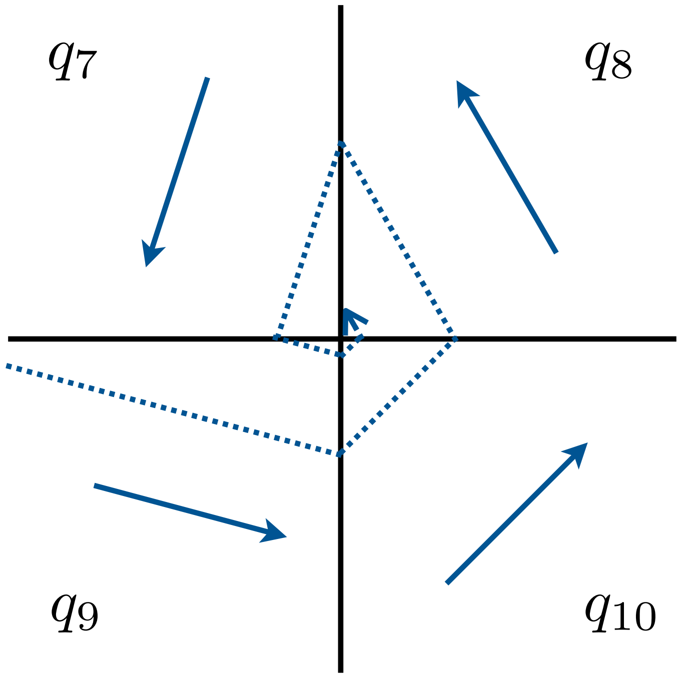
Step 1: AS verification



Concrete system $\mathcal{H}$

- Local analysis is reduced to the switching predicates passing through the equilibrium point.

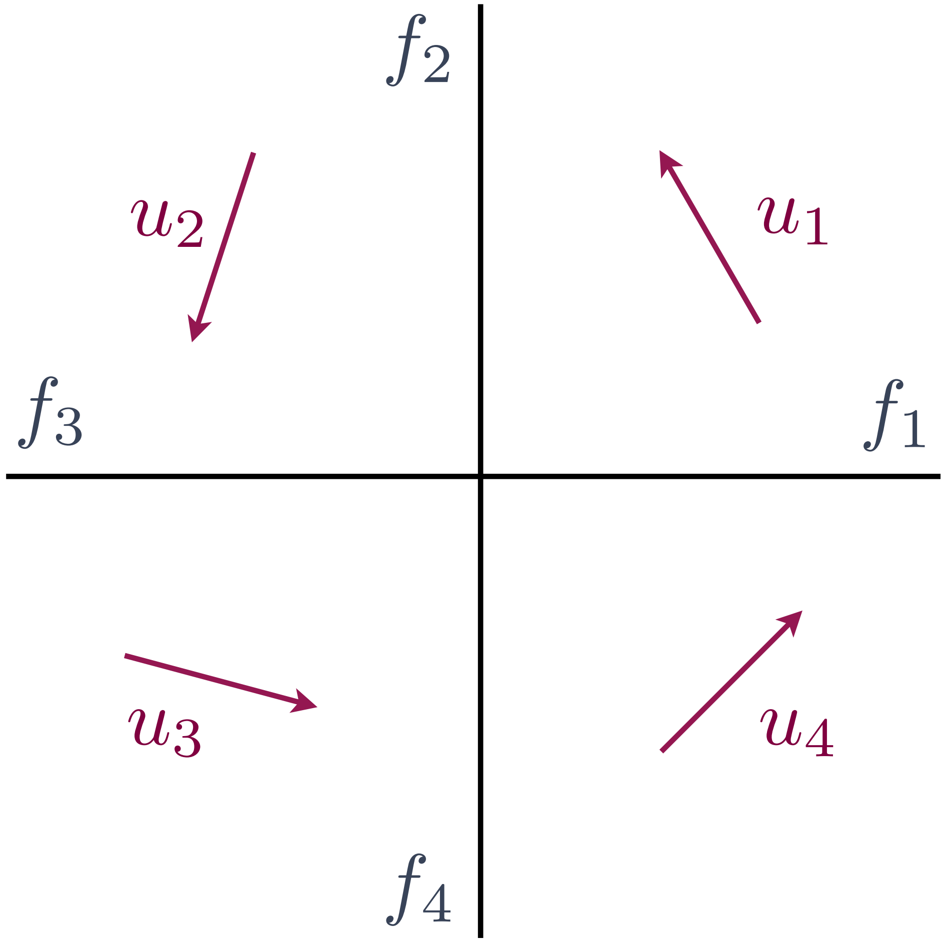
Step 1: AS verification



Concrete system $\mathcal{H}'$

- Local analysis is reduced to the switching predicates passing through the equilibrium point.

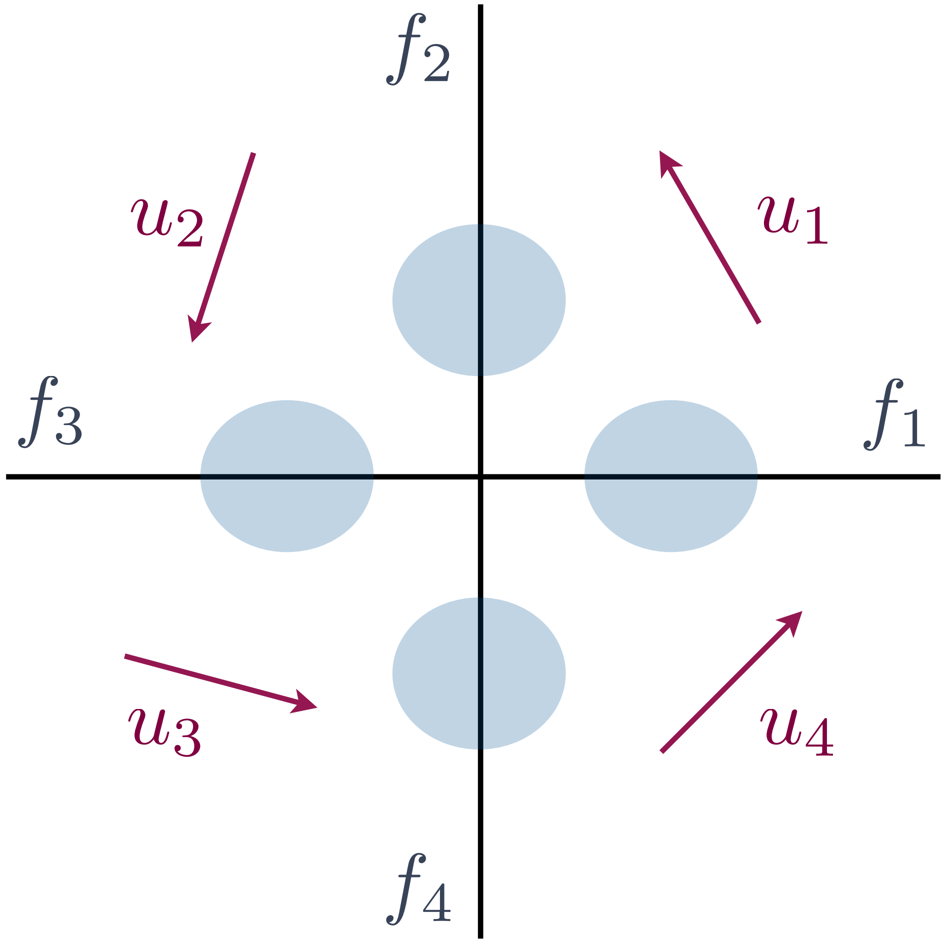
Predicate Abstraction



Concrete system $\mathcal{H}'$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

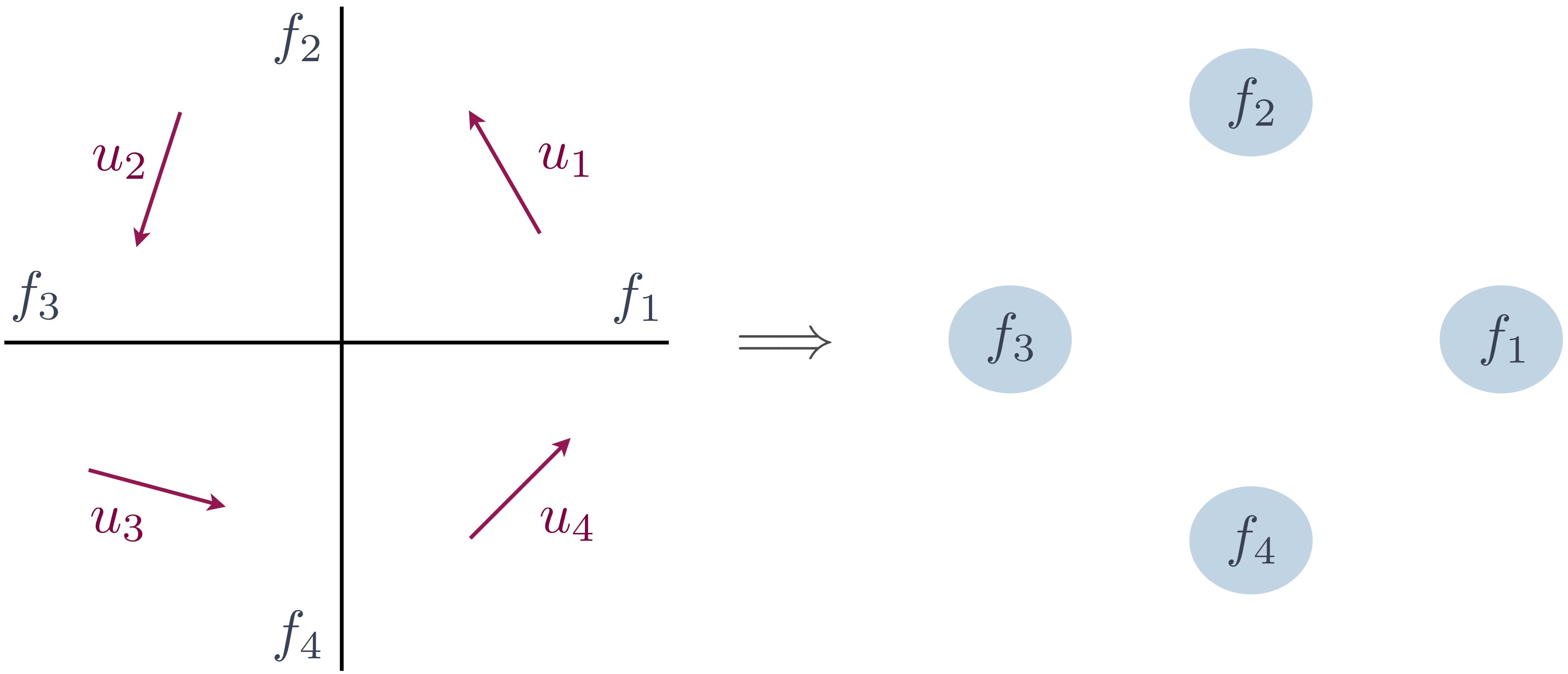
Predicate Abstraction



Concrete system $\mathcal{H}'$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

Predicate Abstraction

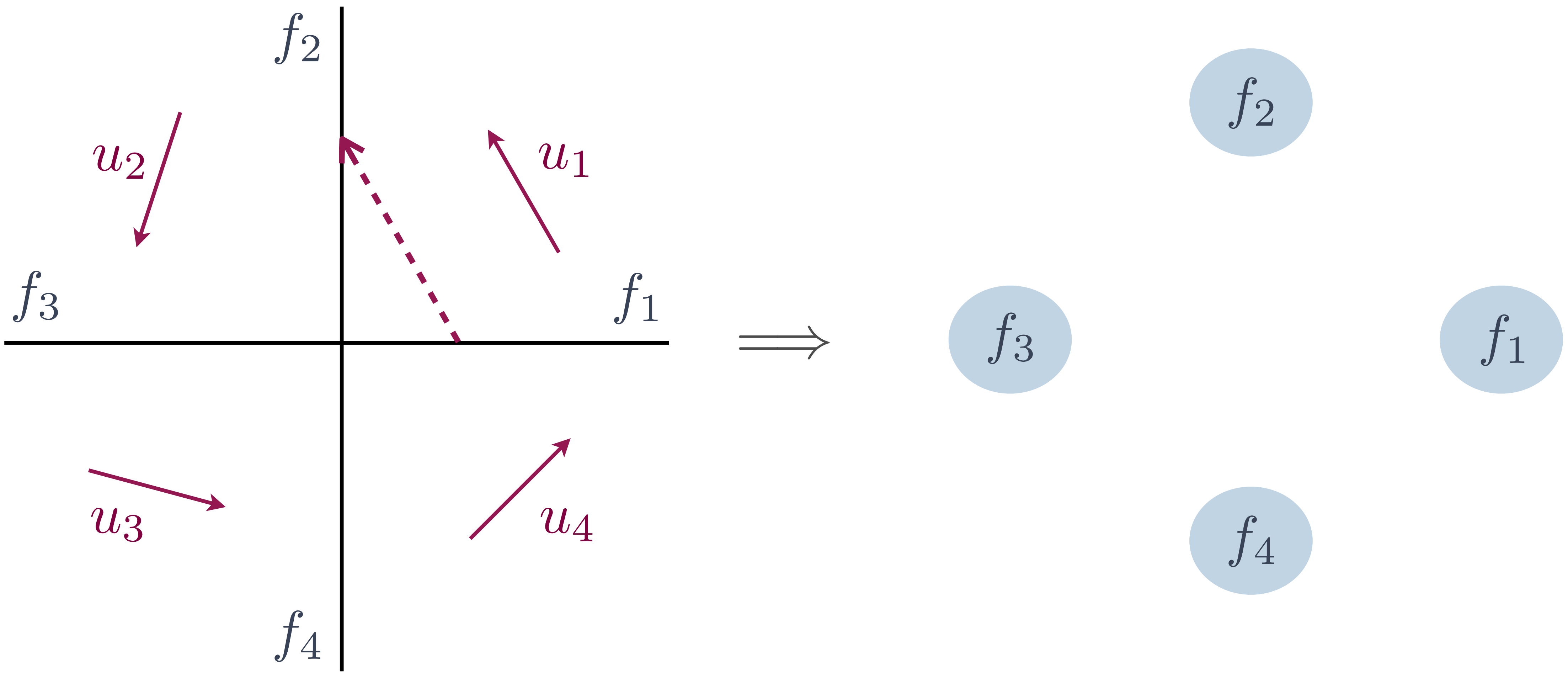


Concrete system $\mathcal{H}'$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

Predicate Abstraction



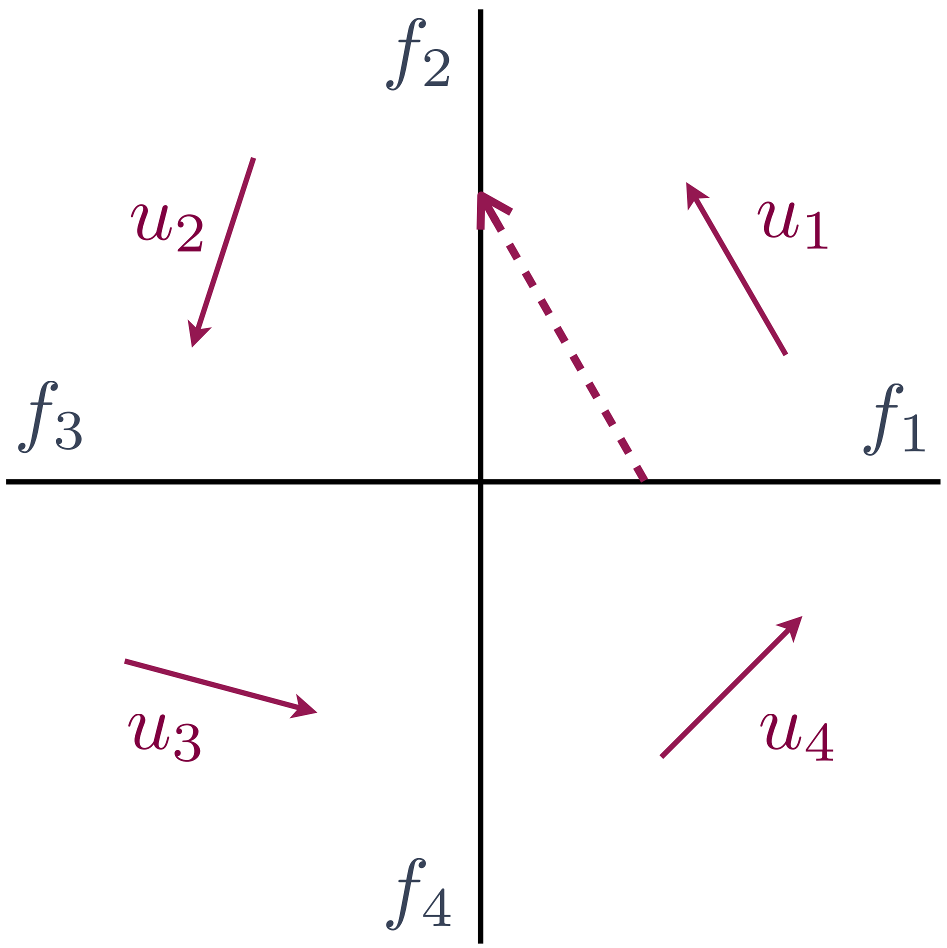
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

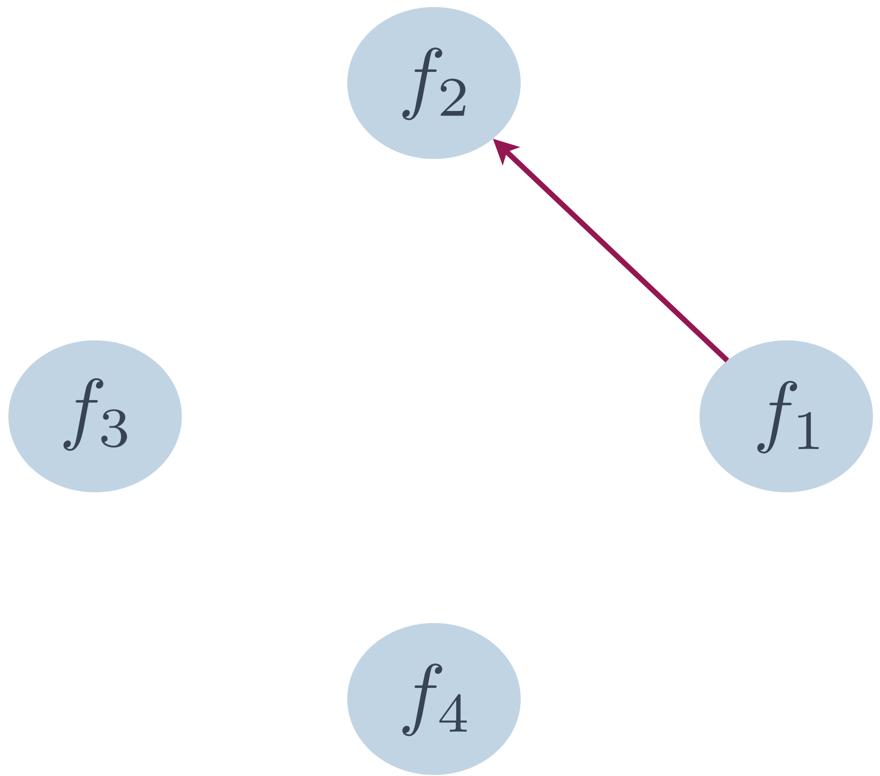
Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.

Predicate Abstraction



$\Longrightarrow$



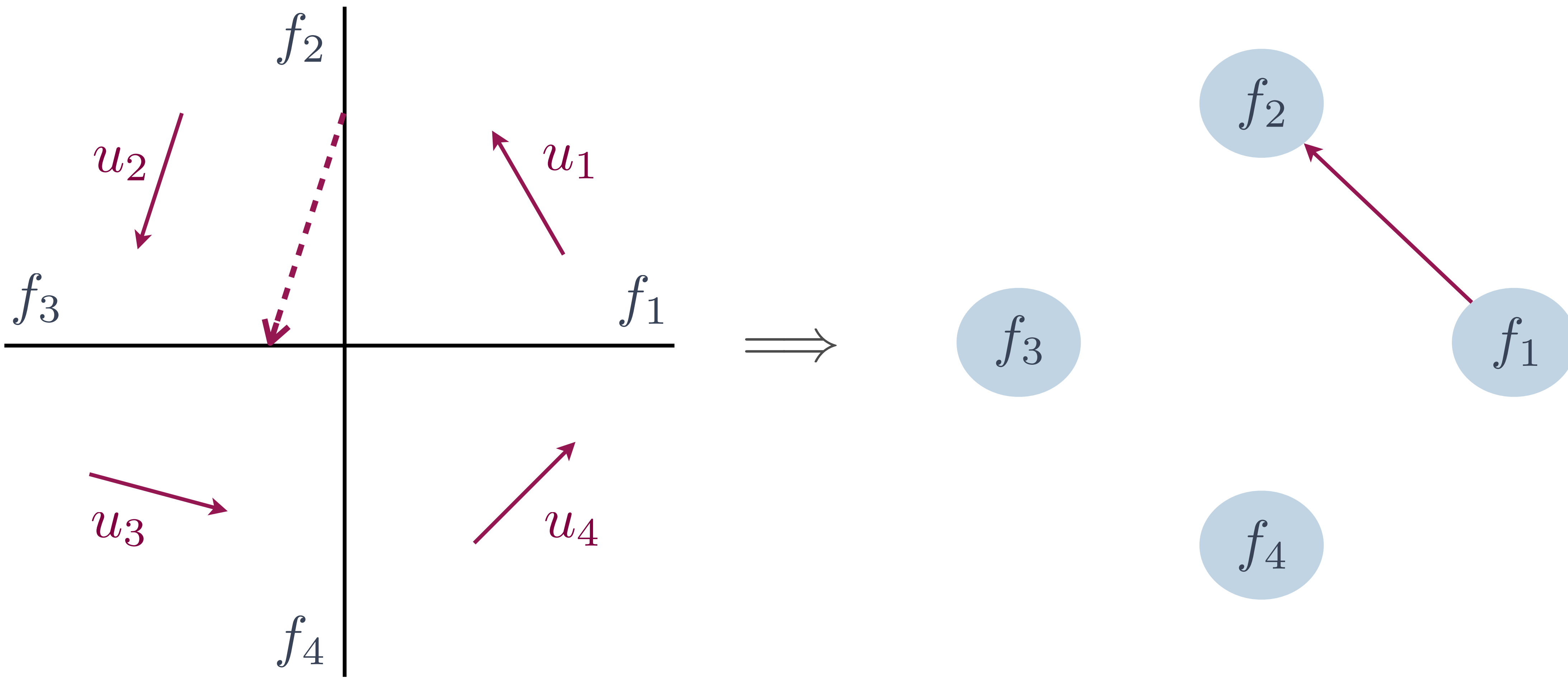
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.

Predicate Abstraction



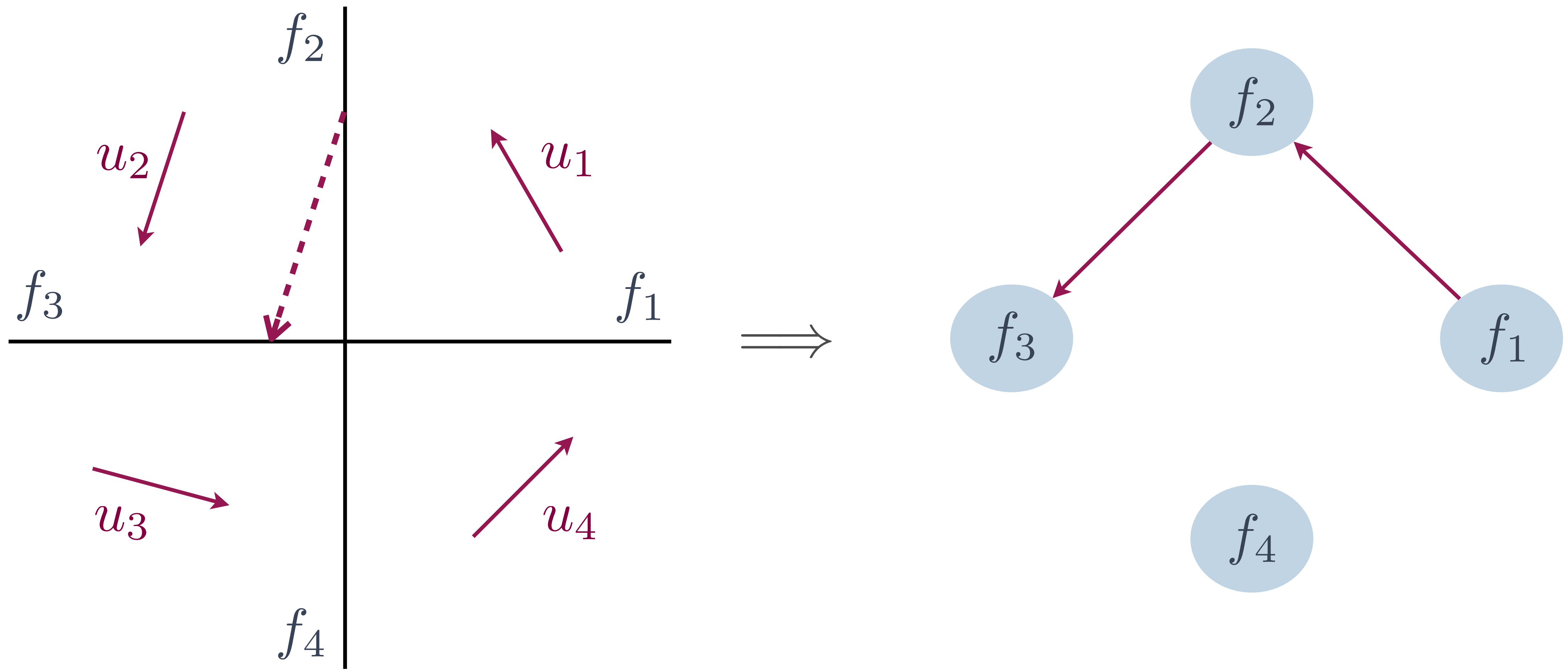
Concrete system $\mathcal{H}'$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

- An edge between facets indicates the existence of an execution.

Predicate Abstraction



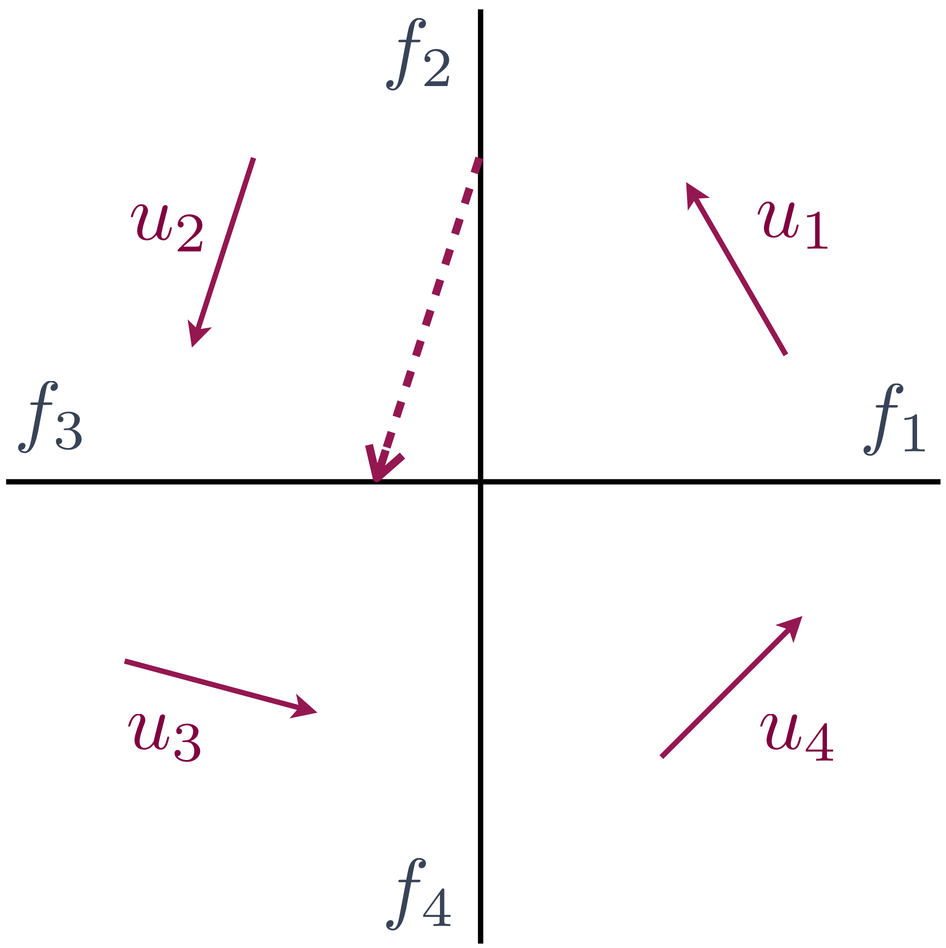
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

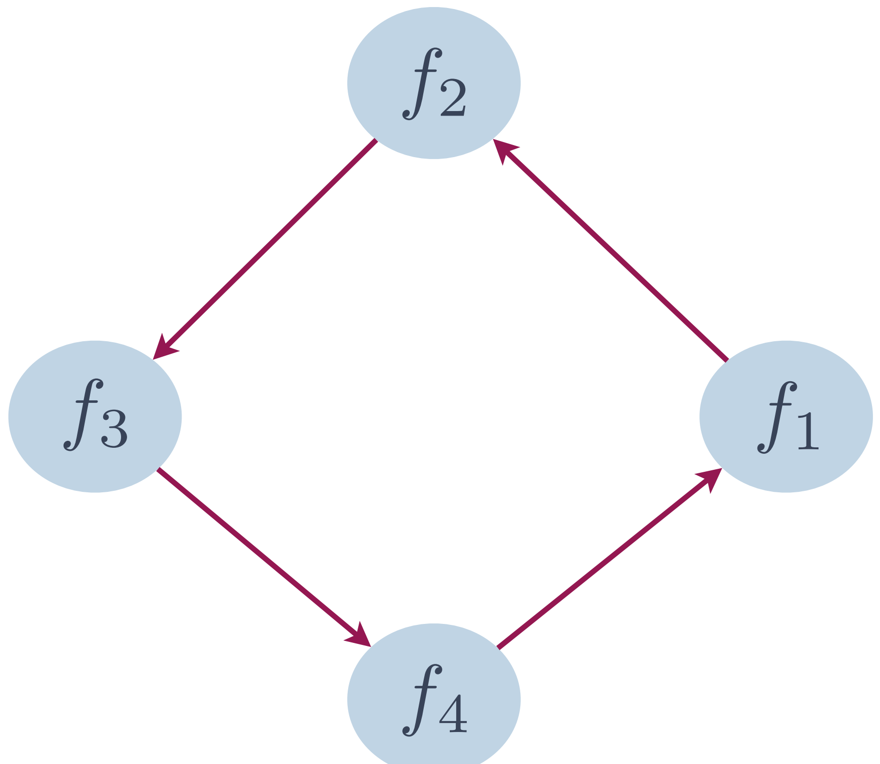
Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.

Predicate Abstraction



$\Longrightarrow$



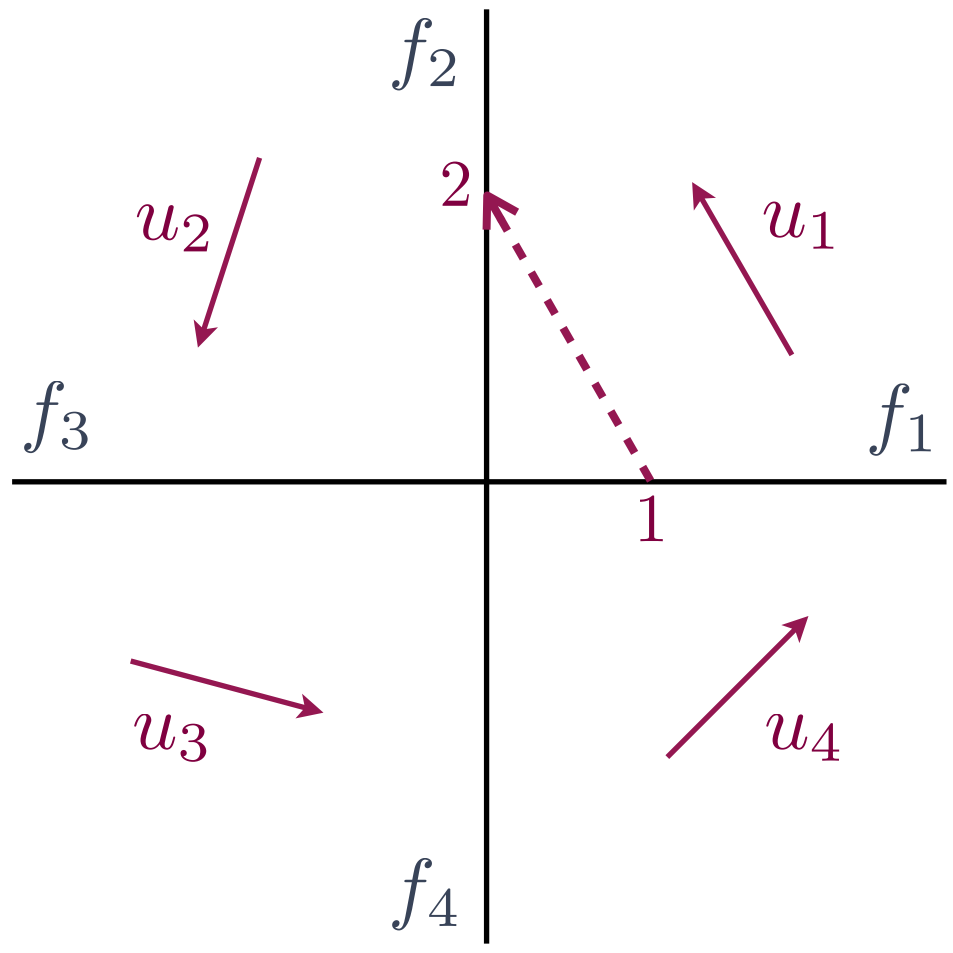
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

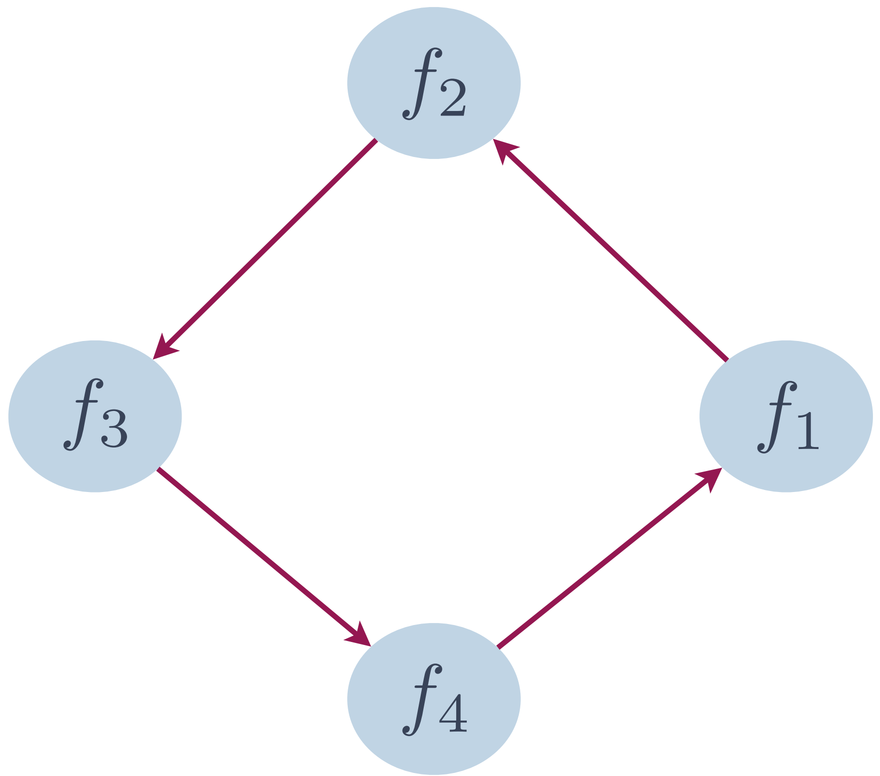
Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.

Quantitative Predicate Abstraction



$\Longrightarrow$



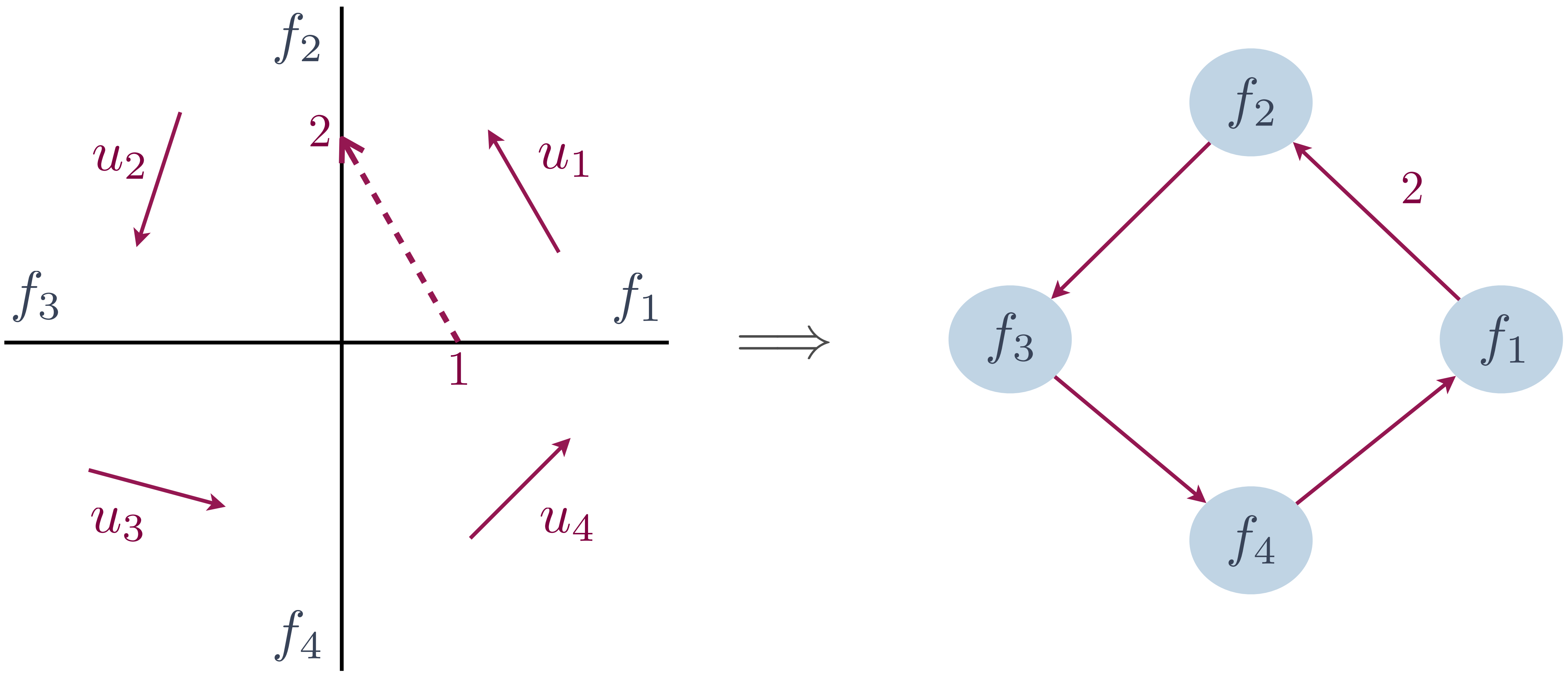
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.
- The weight refers to the variation of distance from equilibrium.

Quantitative Predicate Abstraction



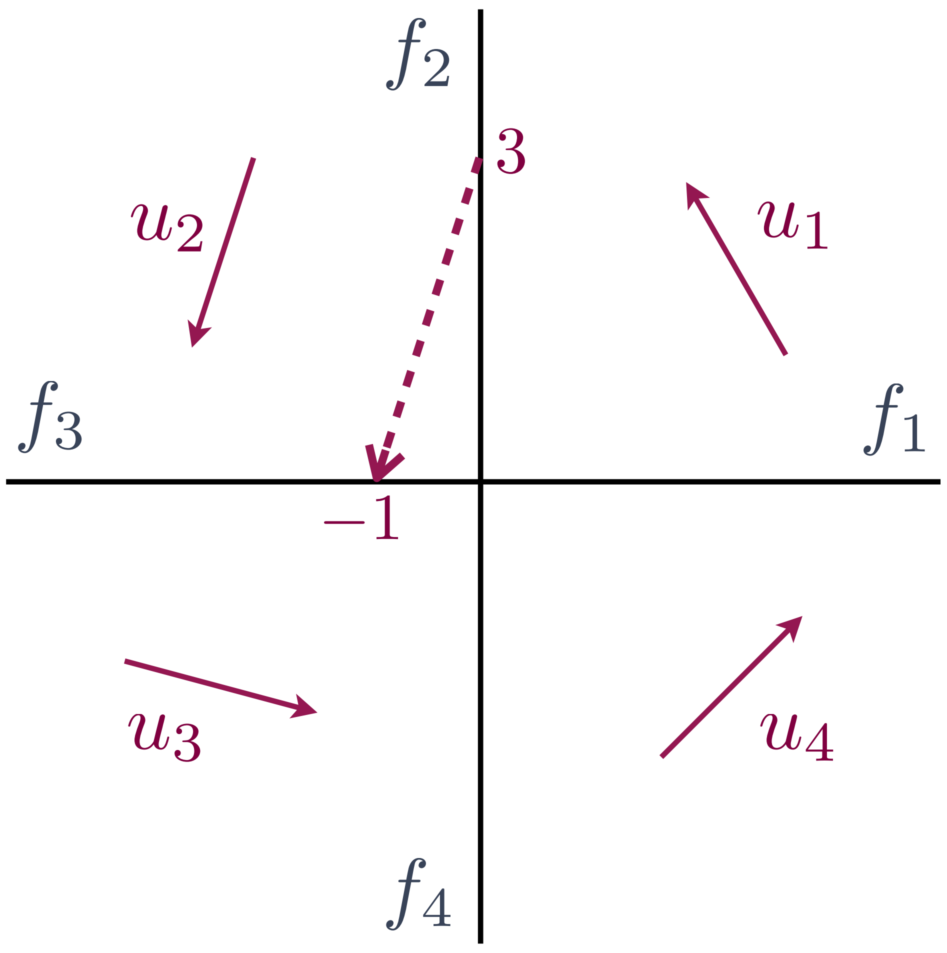
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

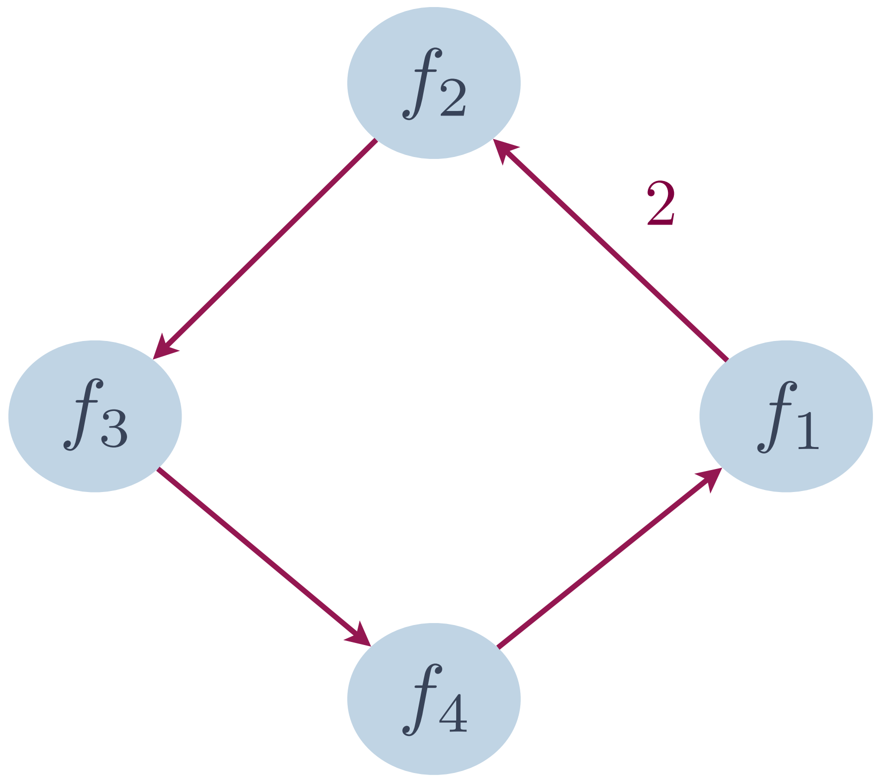
Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.
- The weight refers to the variation of distance from equilibrium.

Quantitative Predicate Abstraction



$\Longrightarrow$



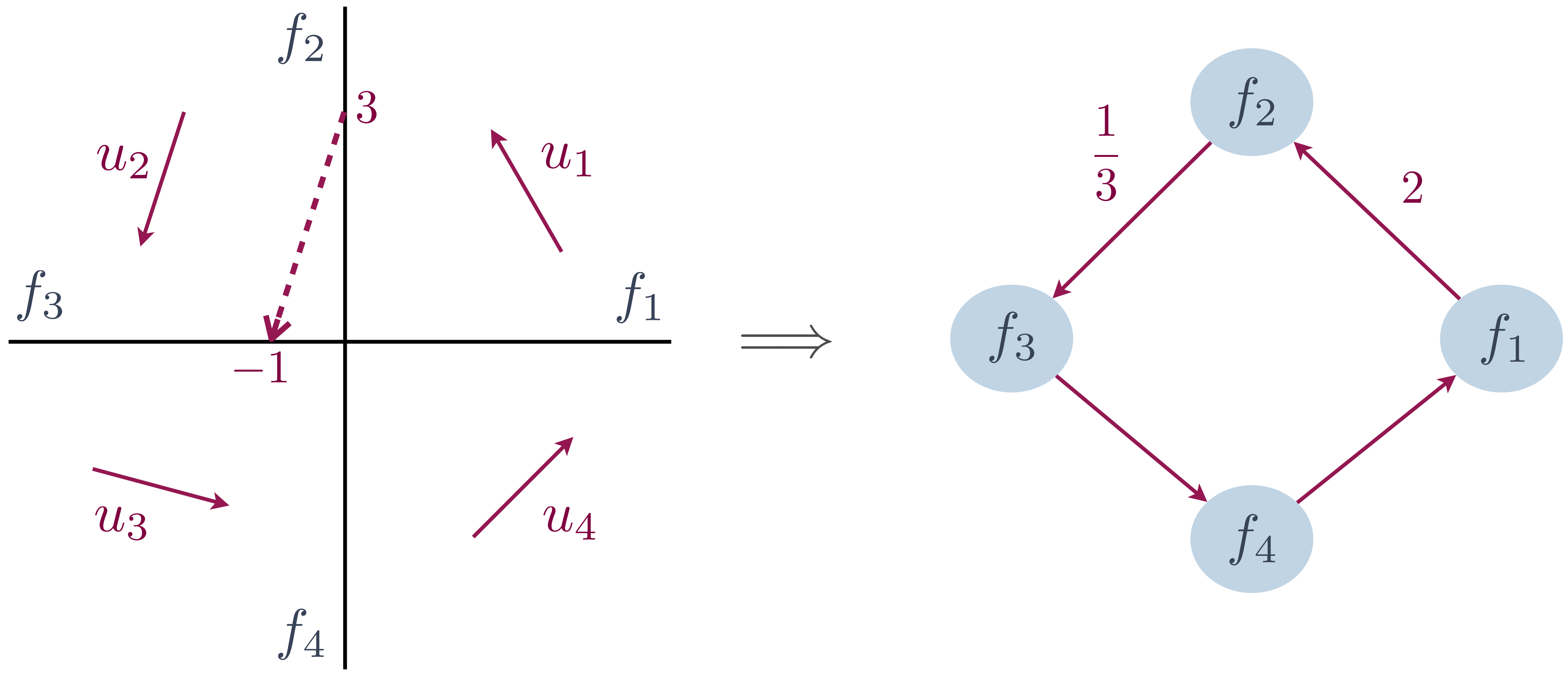
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.
- The weight refers to the variation of distance from equilibrium.

Quantitative Predicate Abstraction



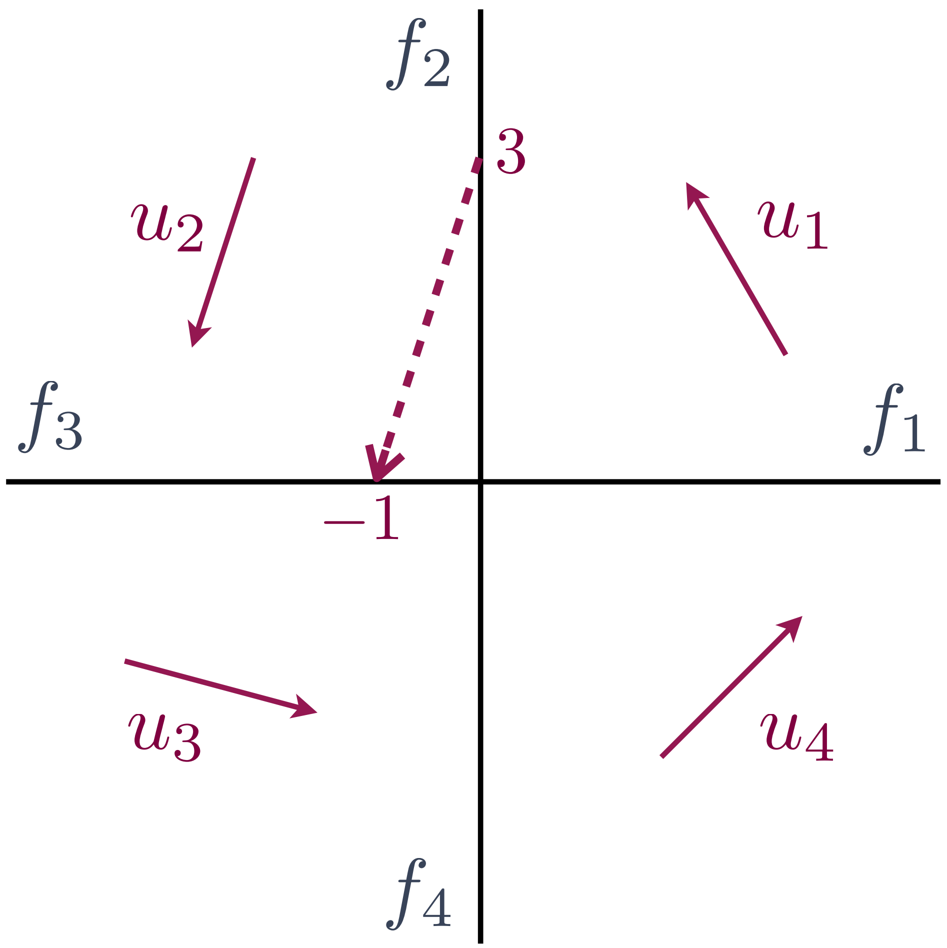
Concrete system $\mathcal{H}'$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

- An edge between facets indicates the existence of an execution.
- The weight refers to the variation of distance from equilibrium.

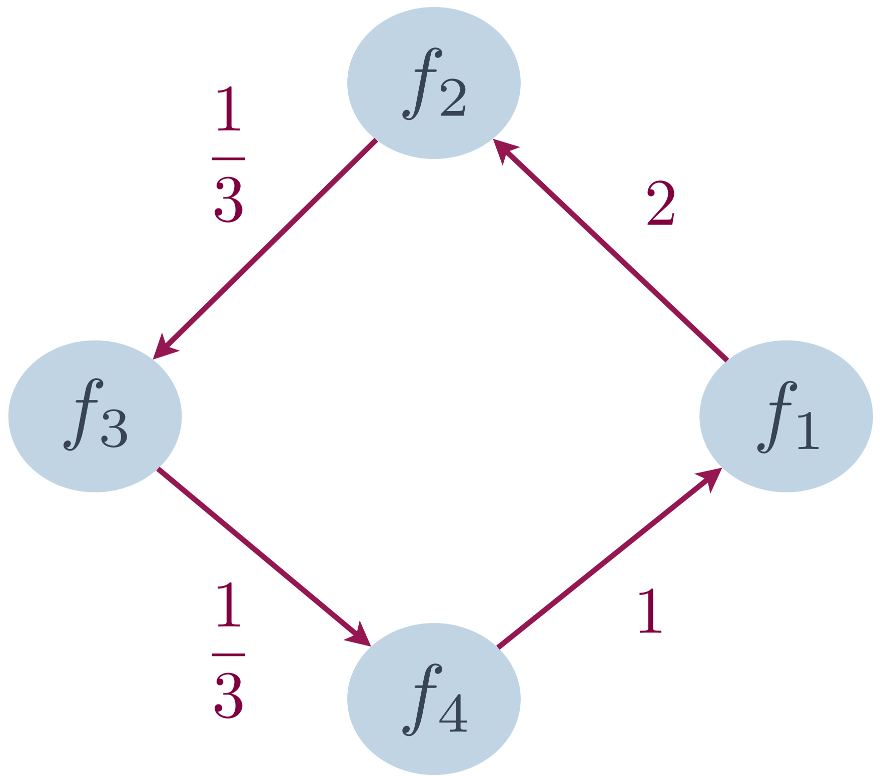
Quantitative Predicate Abstraction



Concrete system $\mathcal{H}'$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

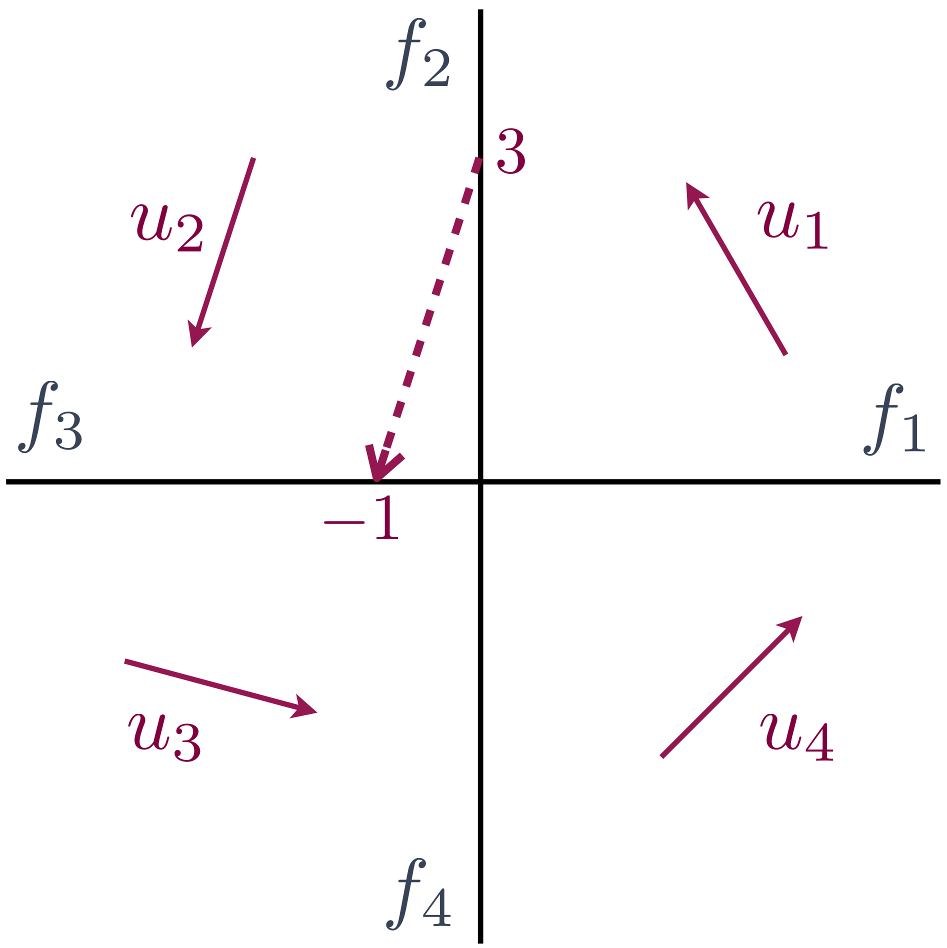
$\Longrightarrow$



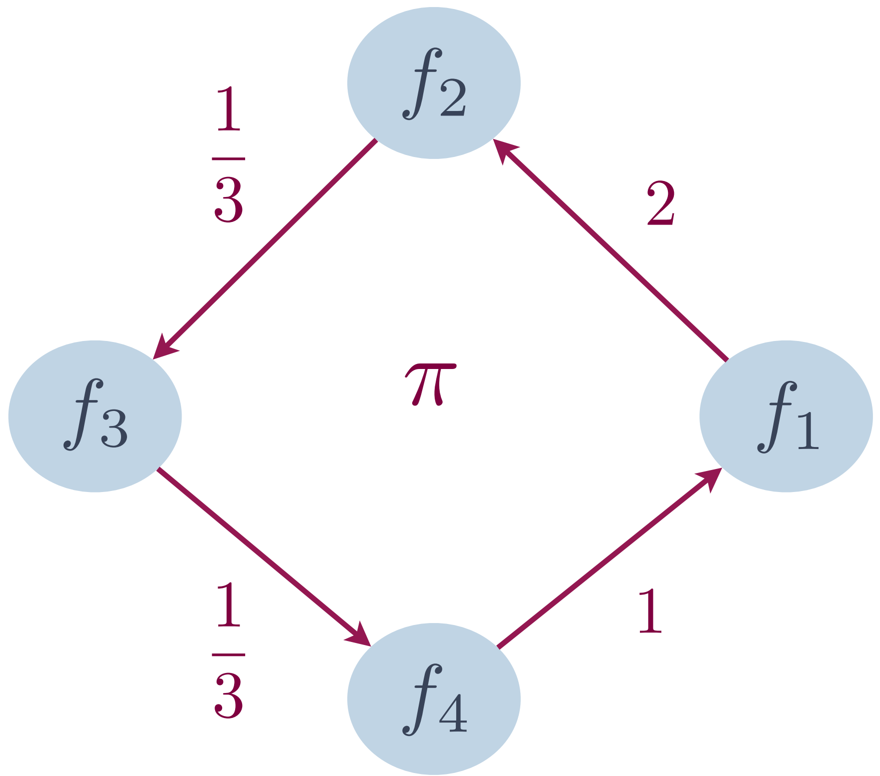
Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

- An edge between facets indicates the existence of an execution.
- The weight refers to the variation of distance from equilibrium.

Quantitative Predicate Abstraction



$\Longrightarrow$



Concrete system $\mathcal{H}'$

Facets $\mathcal{F} = \{f_1, f_2, f_3, f_4\}$

Abstract system $\mathcal{A}(\mathcal{H}', \mathcal{F})$

$$W(\pi) = 2 \cdot \frac{1}{3} \cdot \frac{1}{3} \cdot 1 = \frac{2}{9} < 1$$

- An edge between facets indicates the existence of an execution.
- The weight refers to the variation of distance from equilibrium.

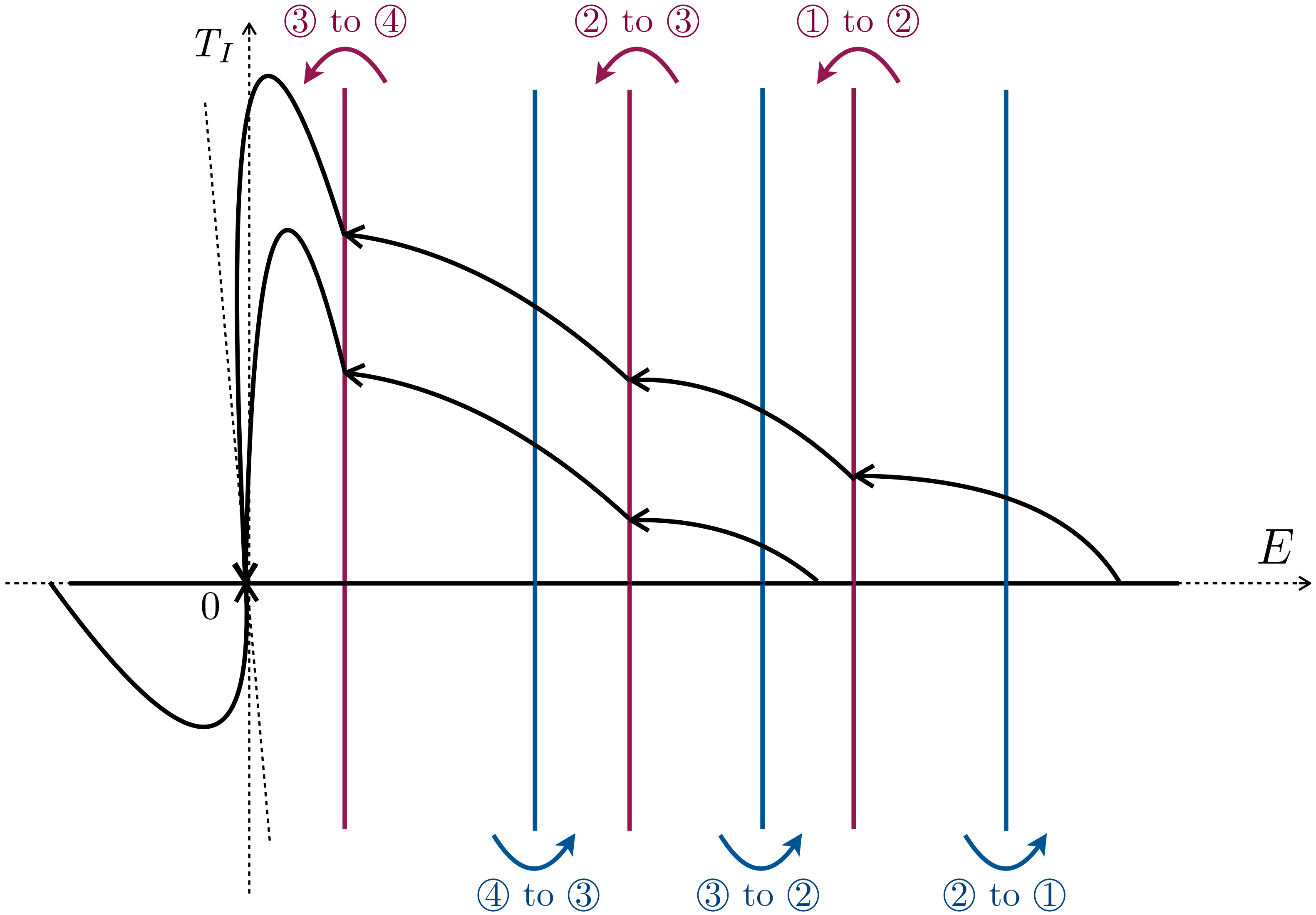
Model-checking

Theorem (Soundness)

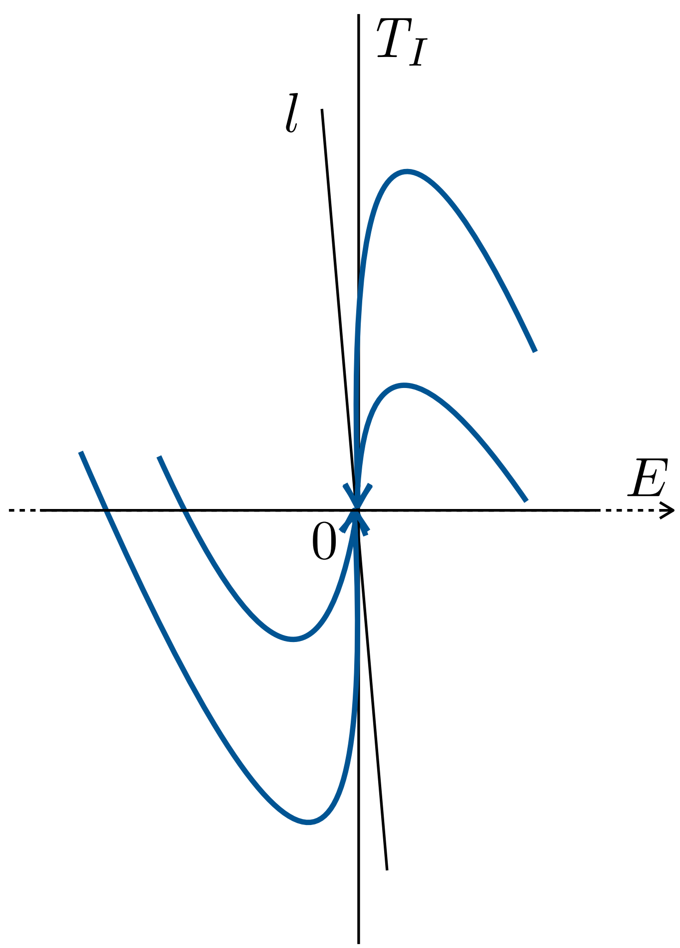
Let $\mathcal{A}(\mathcal{H}, \mathcal{F})$ be a quantitative abstraction. The hybrid system $\mathcal{H}$ is asymptotically stable if:

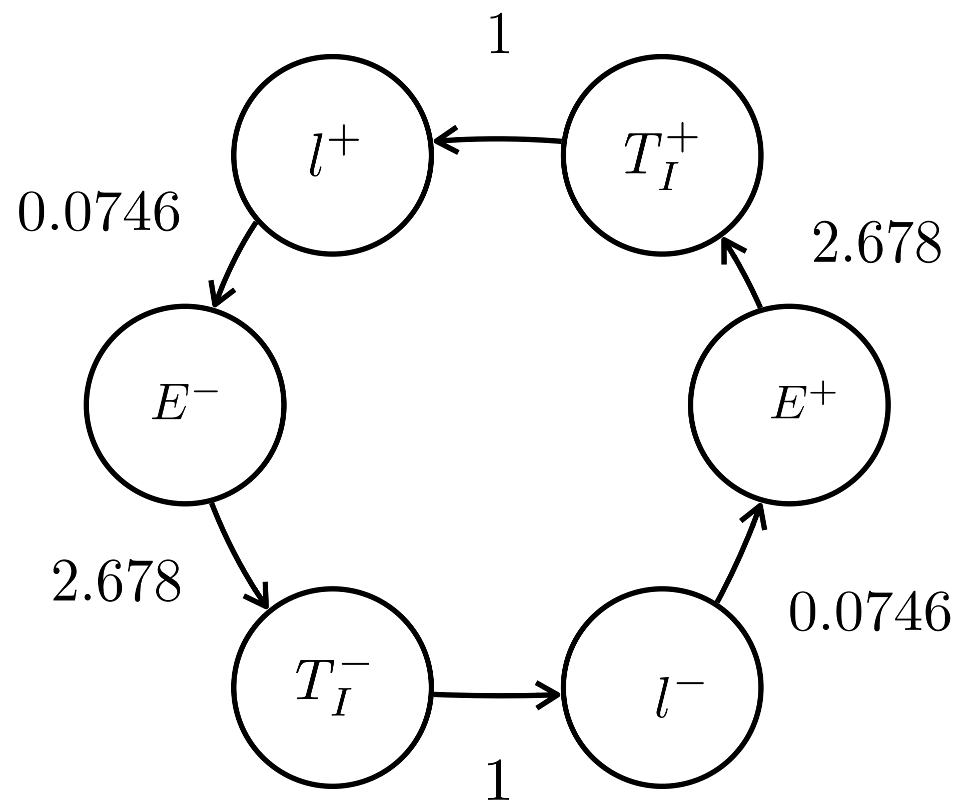
- All executions which eventually remain in a region converge to the origin.
- Every simple cycle has product of weights on the edges less than 1.

AS verification for the gearbox



AS verification for the gearbox

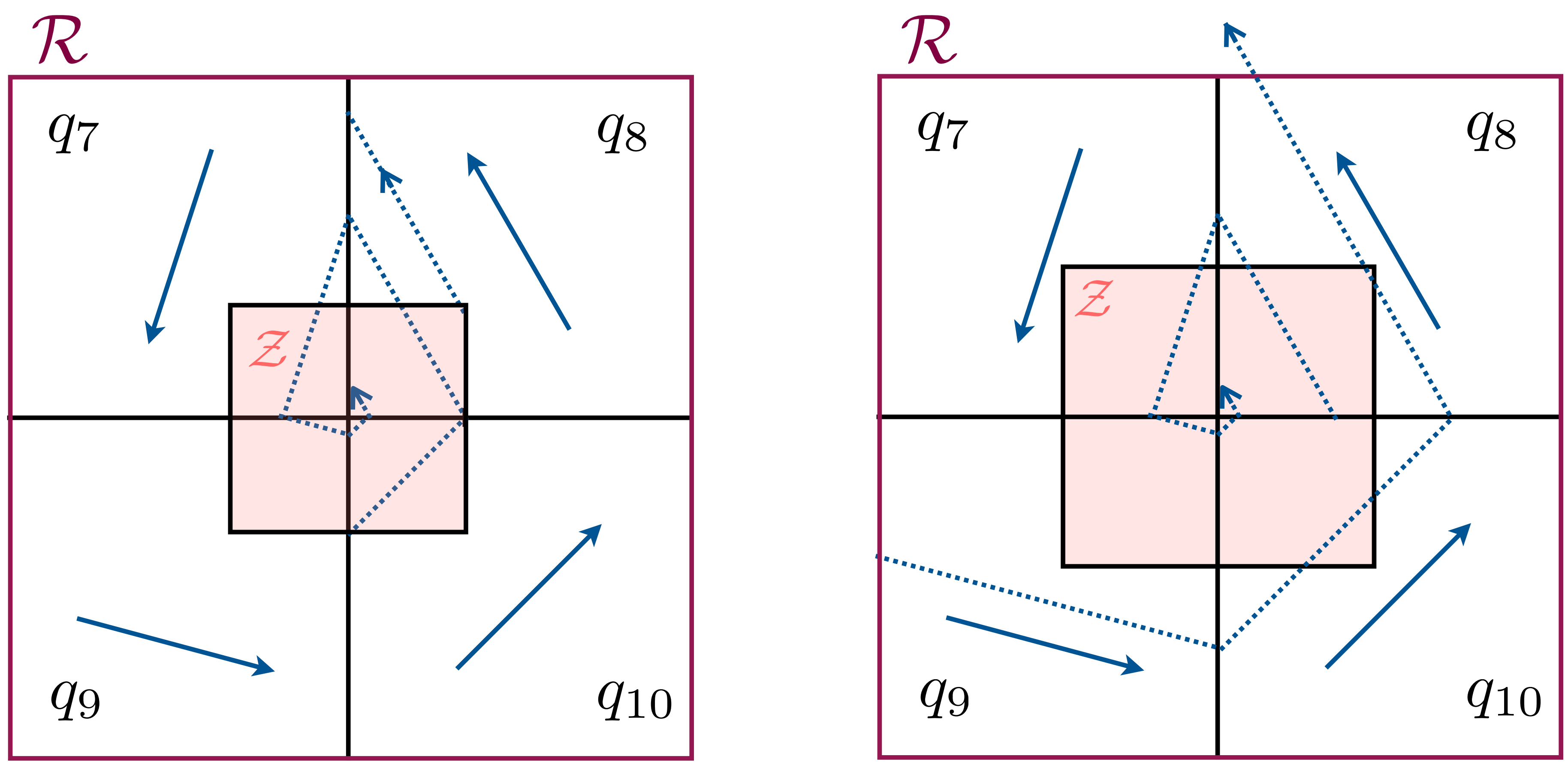




$$W(\pi) = 0.0746 \cdot 2.678 \cdot 1 \cdot 0.0746 \cdot 2.678 \cdot 1 = 0.03991 < 1 \quad \Rightarrow \quad \text{AS}$$

Step 2: Stability zone computation

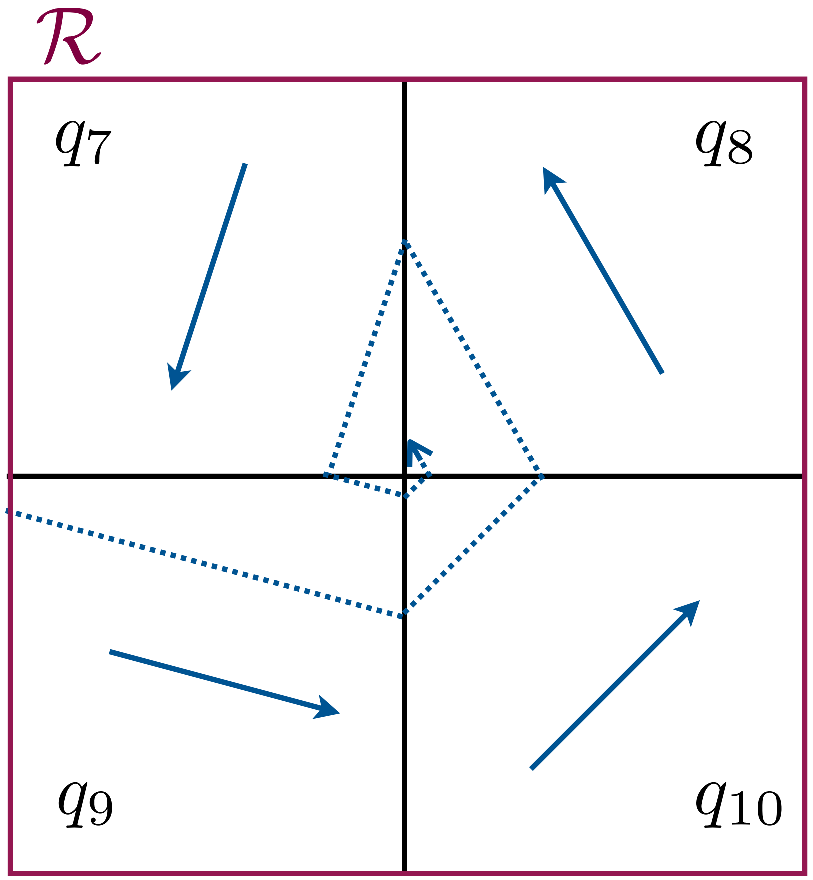
$\mathcal{Z} \subseteq \mathcal{R}$ is a **stability zone** with respect to $\mathcal{R}$ if every execution starting at $\mathcal{Z}$ will remain forever inside $\mathcal{R}$.



Stability zone Not stability zone

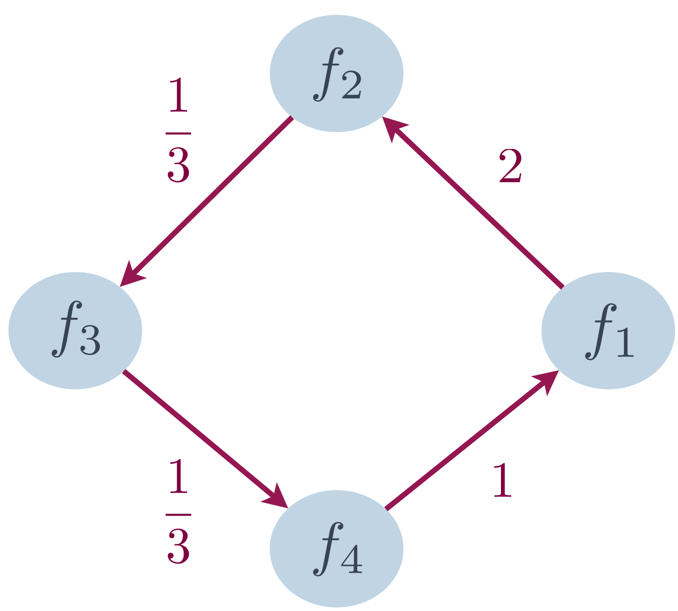
Stability zone computation

- Center region $\mathcal{R}$ of $\mathcal{H}$

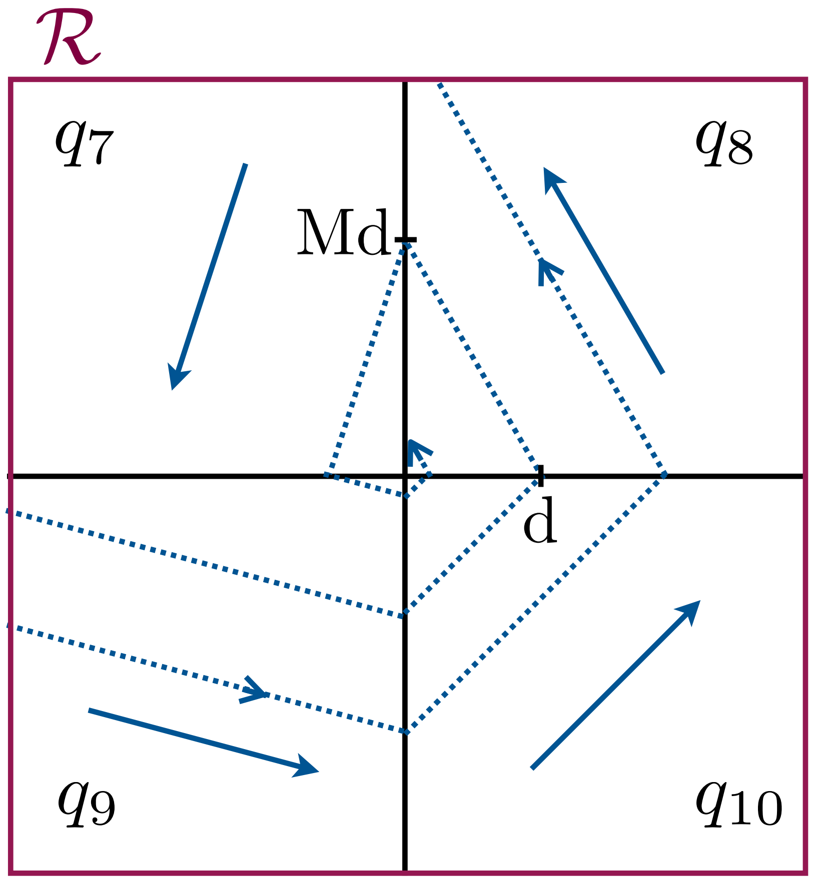


Stability zone computation

- Center region $\mathcal{R}$ of $\mathcal{H}$
- M = max {1, W(π): π path in $\mathcal{A}(\mathcal{H}, \mathcal{F})$}

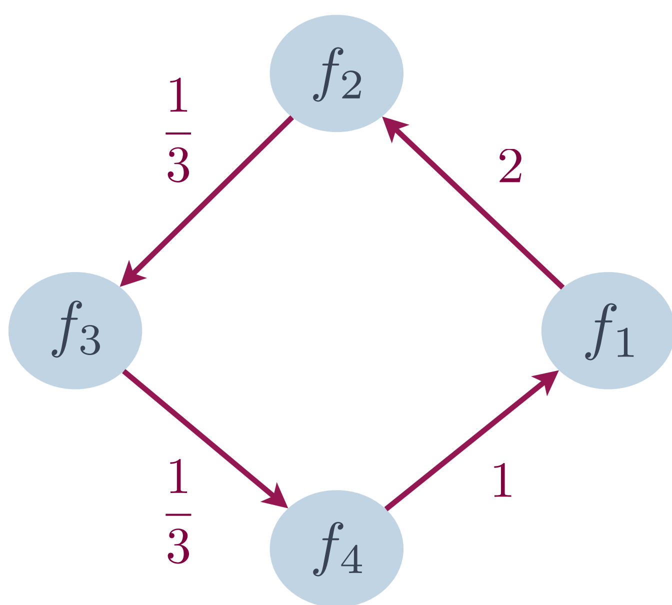


M = 2

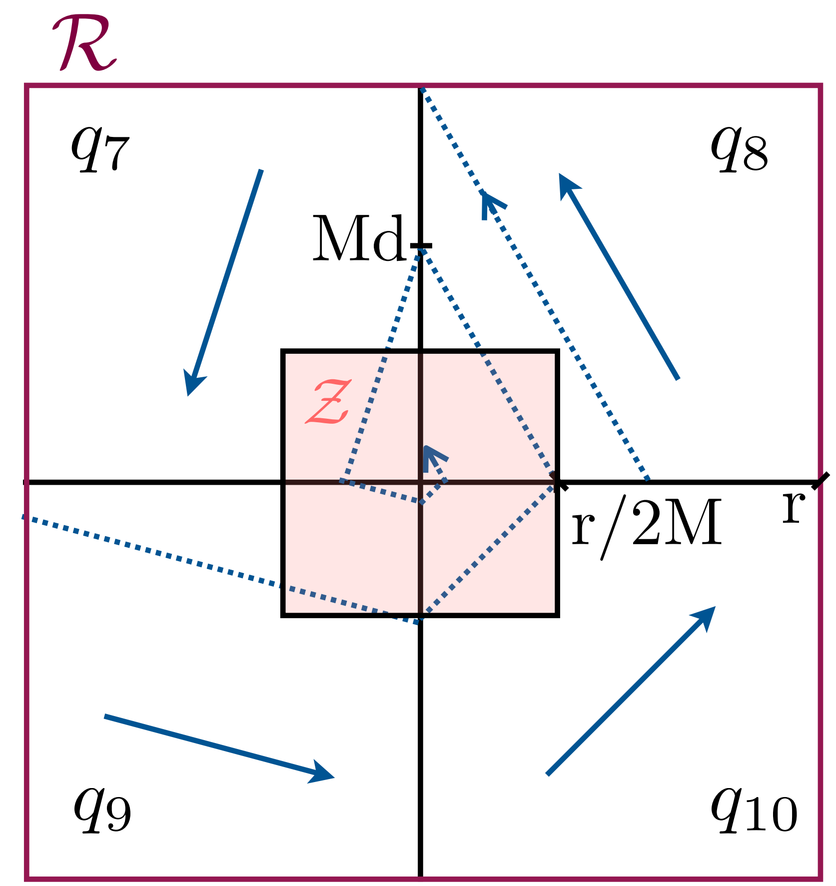


Stability zone computation

- Extract the center region $\mathcal{R}$ of $\mathcal{H}$
- M = max {1, W(π): π path in $\mathcal{A}(\mathcal{H}, \mathcal{F})$}

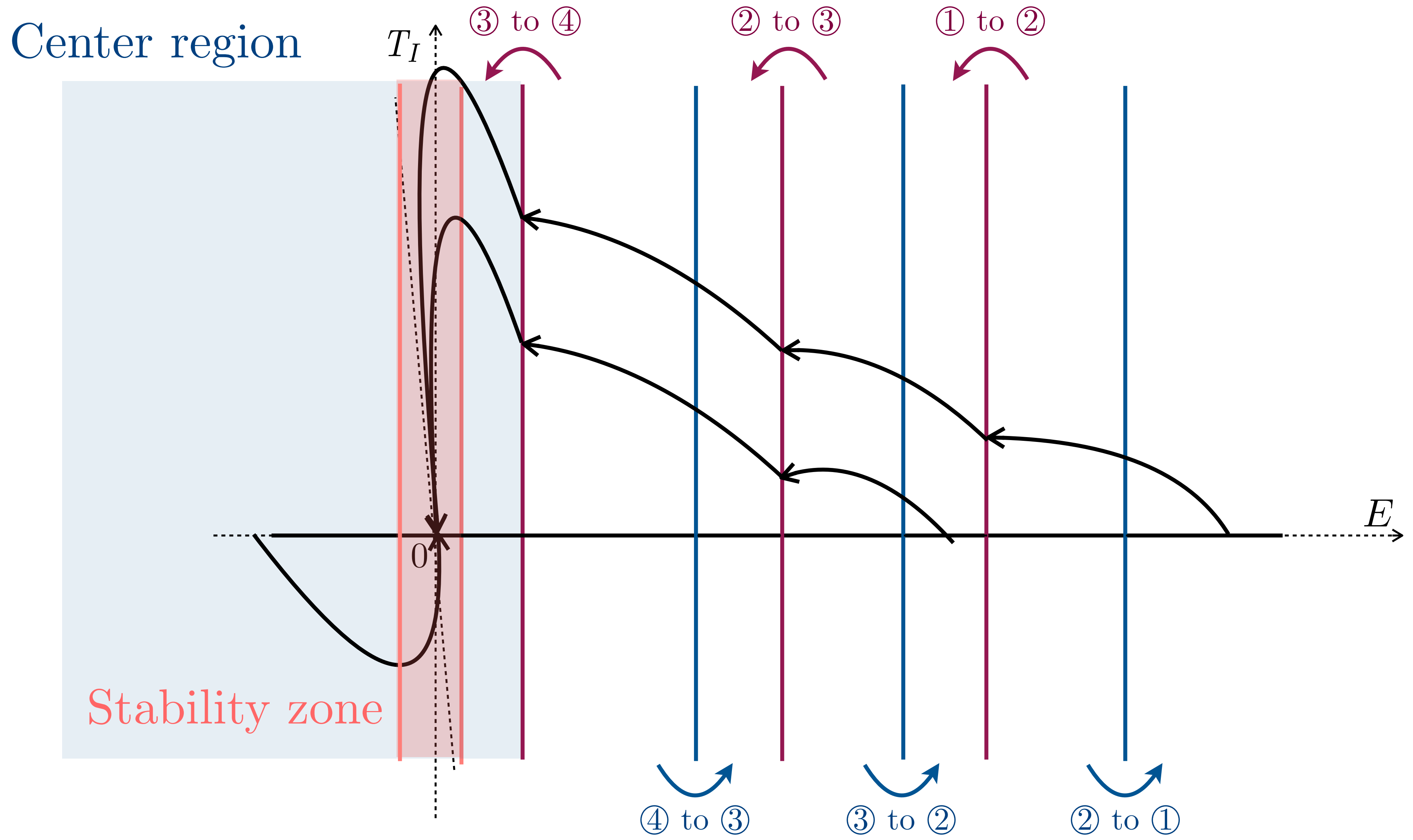


M = 2



- Shrink the center region by a factor of M: $\mathcal{Z}$

Stability zone computation for the gearbox

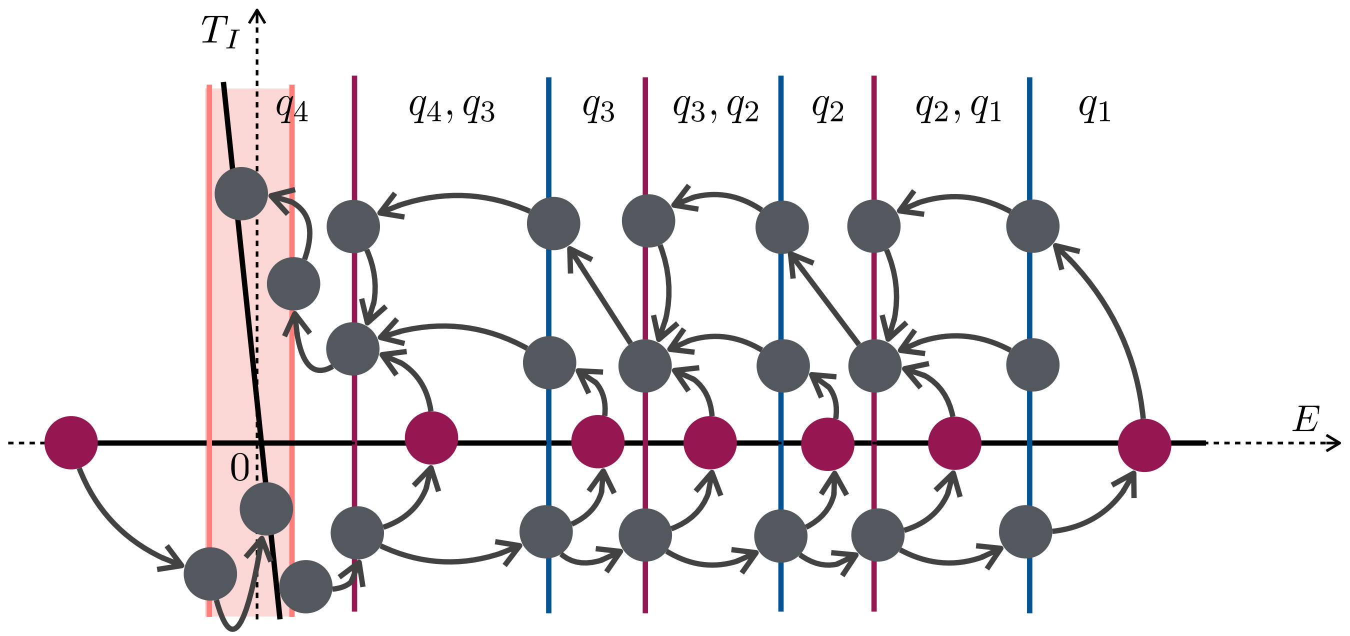


Step 3: RS verification

- Quantitative predicate abstraction.
- Graph transformation.
- Termination analysis.

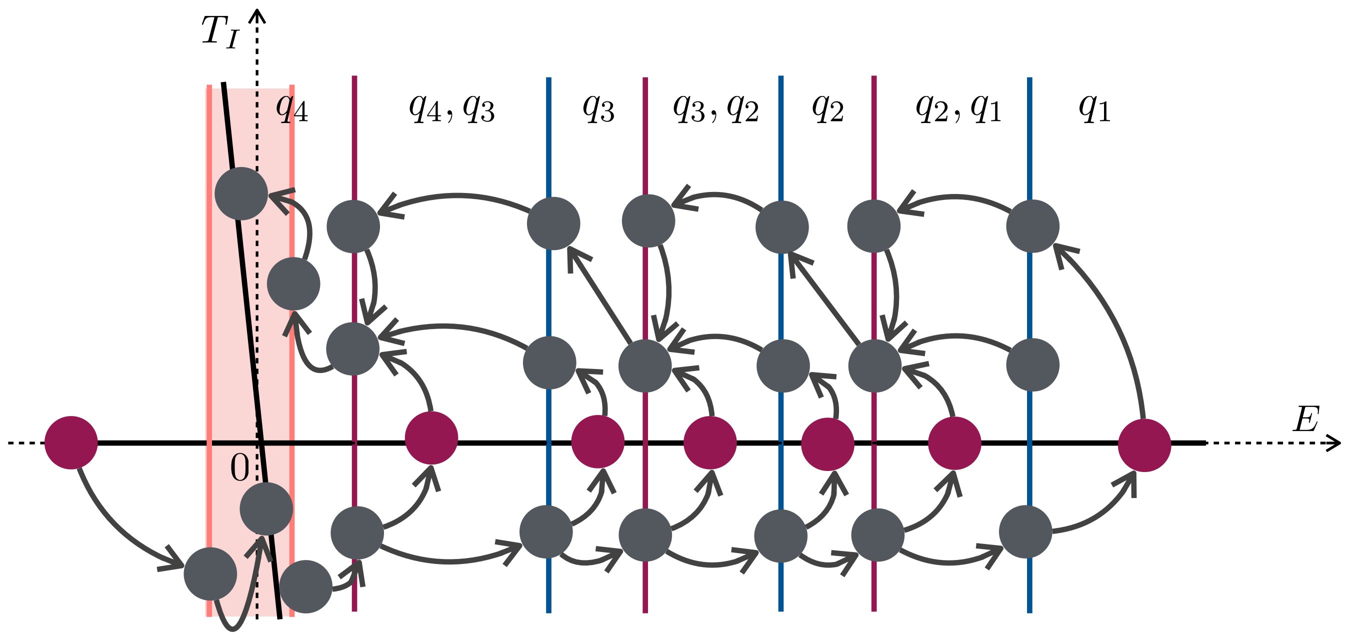
RS verification for the gearbox

Quantitative Predicate Abstraction



RS verification for the gearbox

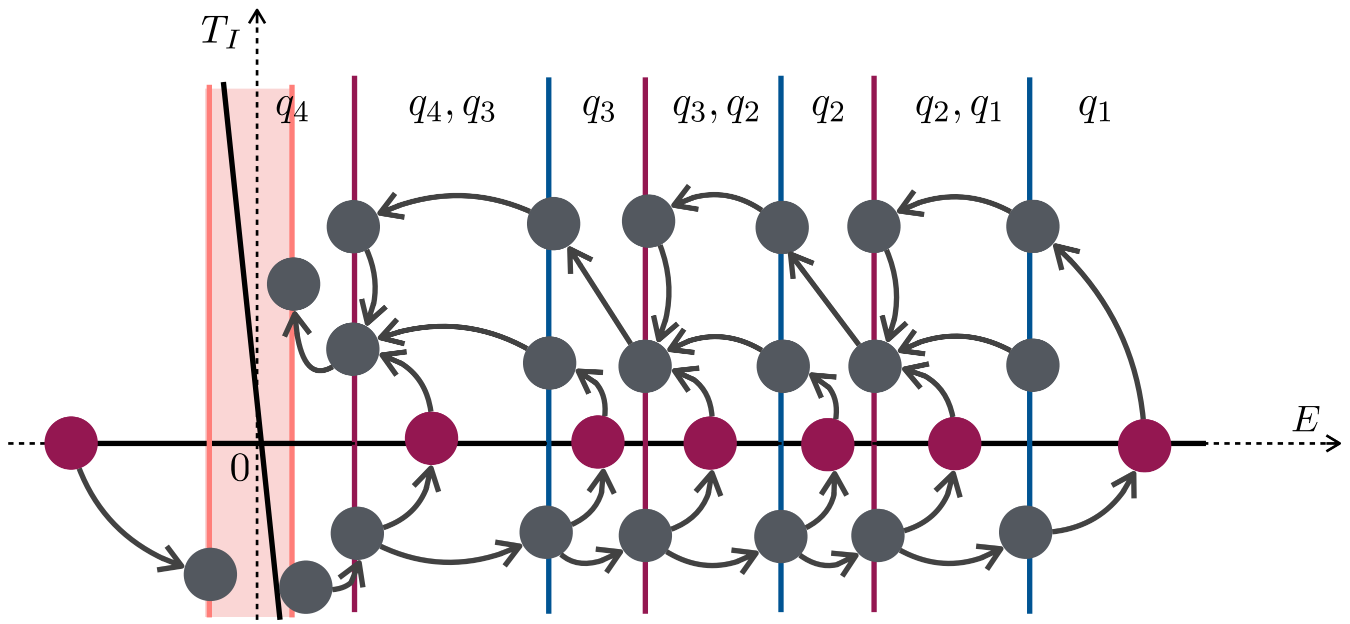
Graph Transformation



RS verification for the gearbox

Graph Transformation

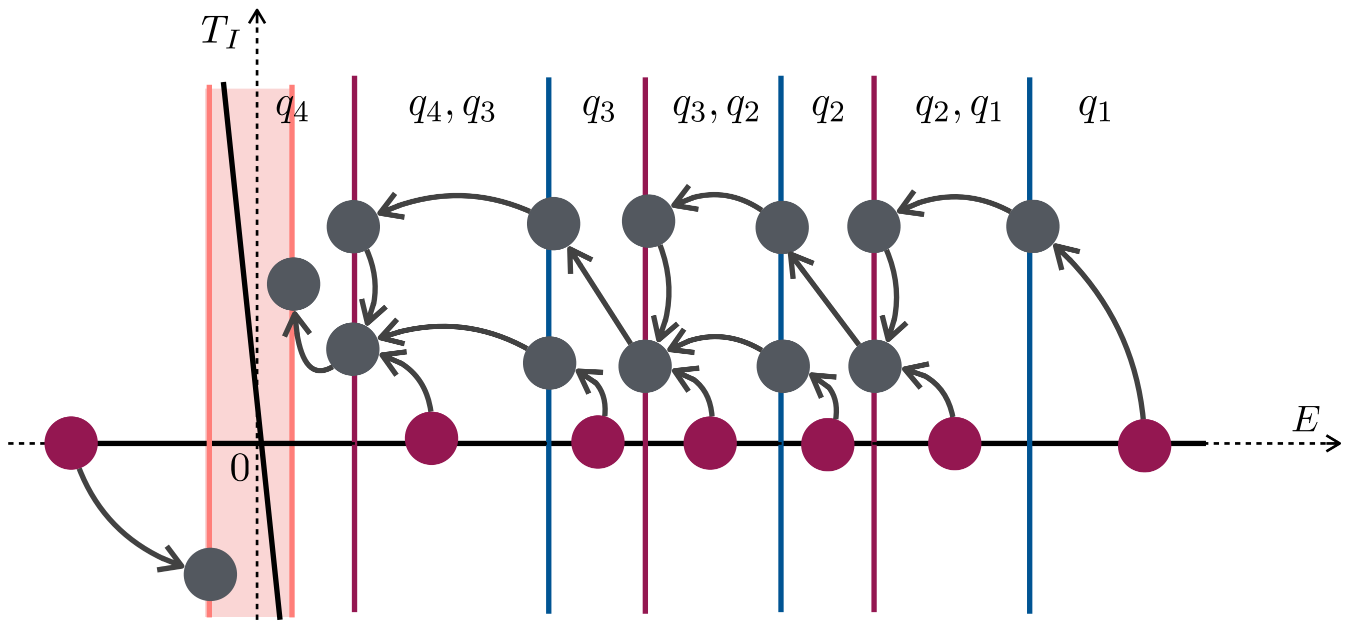
- Delete nodes in the interior of stability zone.



RS verification for the gearbox

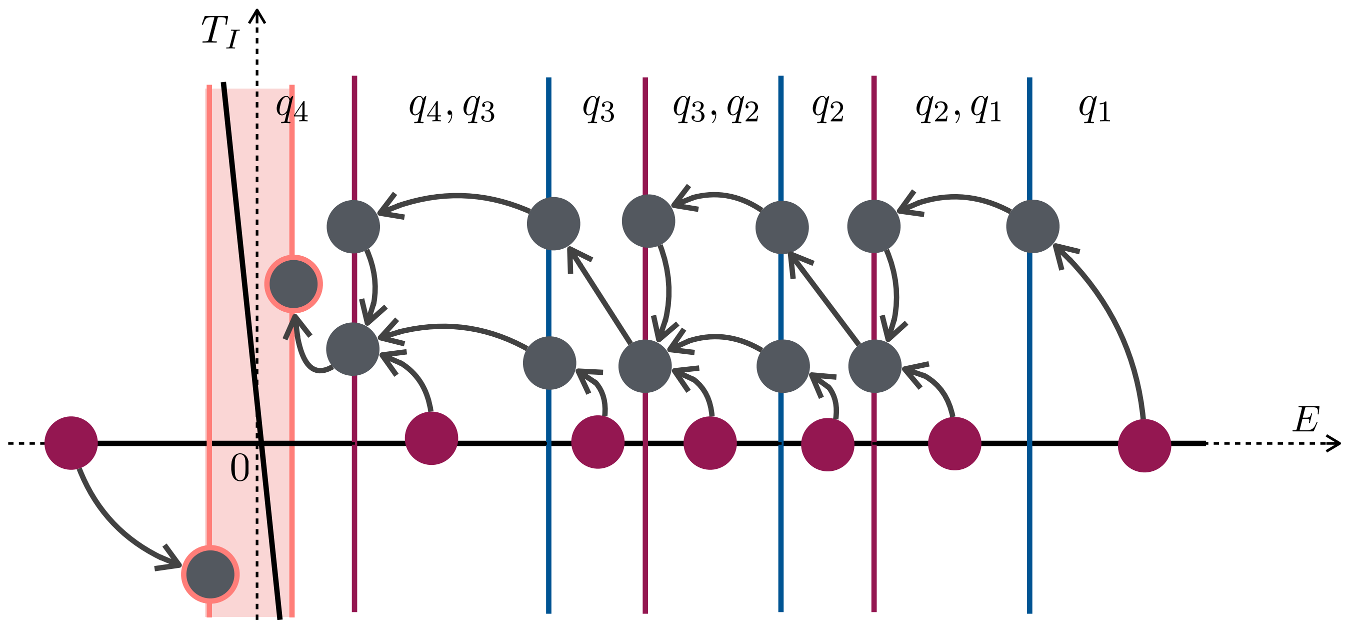
Graph Transformation

- Delete nodes in the interior of stability zone.
- Delete non-reachable nodes from initial nodes.



RS verification for the gearbox

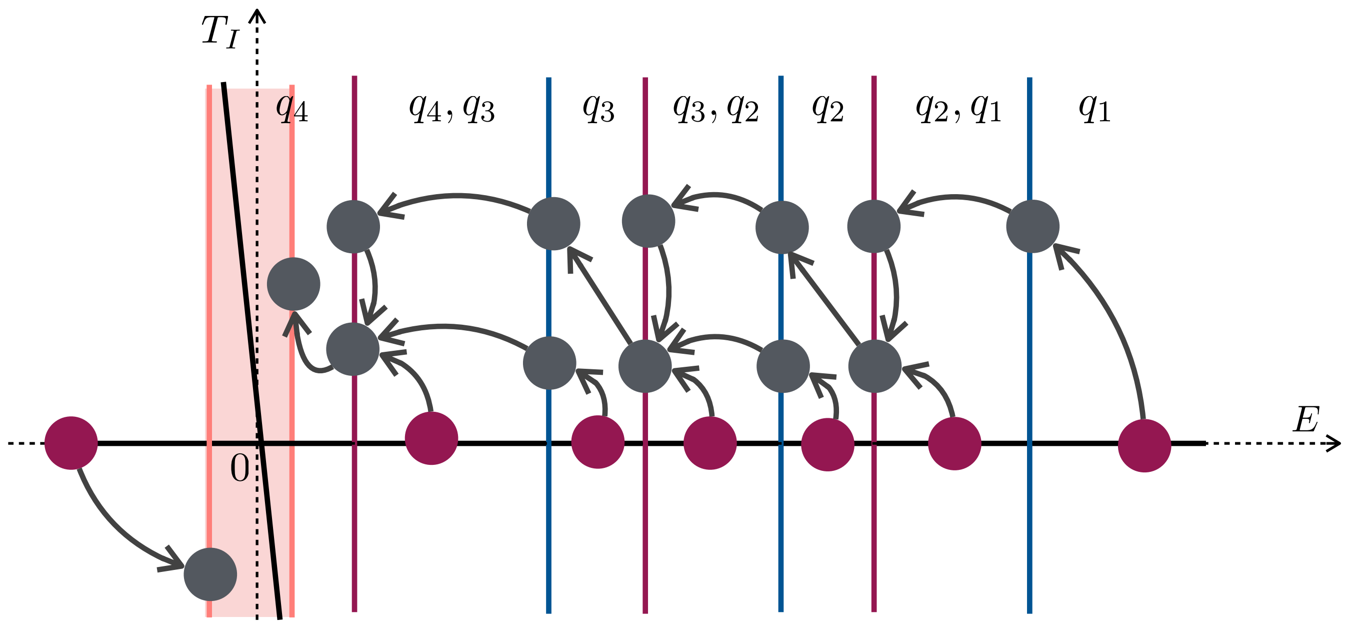
Termination Analysis



RS verification for the gearbox

Termination Analysis

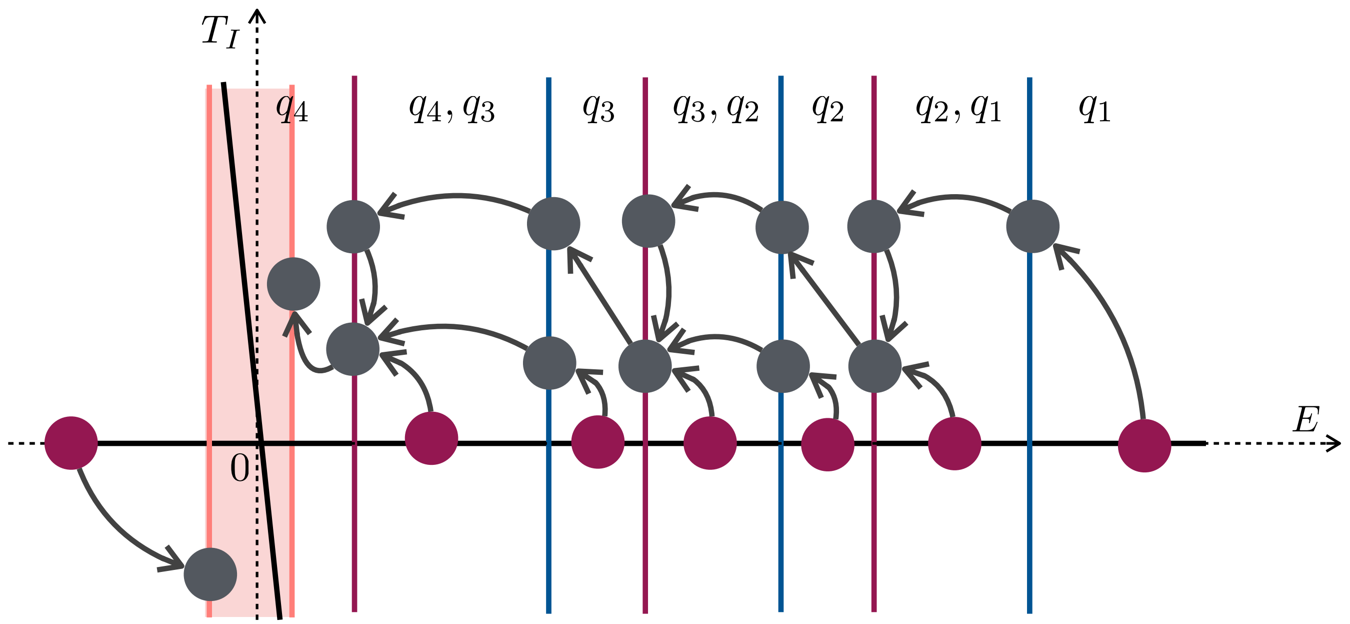
- Existence of an edge with weight $\infty \Rightarrow$ RS False.



RS verification for the gearbox

Termination Analysis

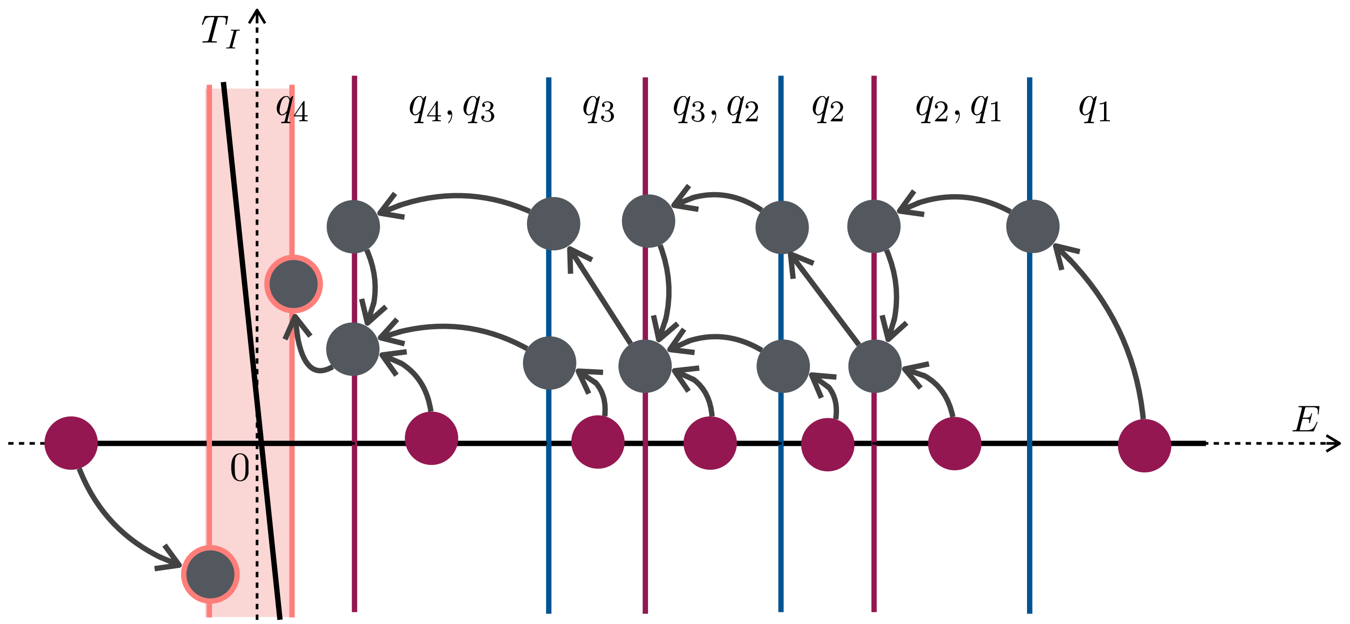
- Existence of an edge with weight $\infty \Rightarrow$ RS False.
- Existence of a cycle $\Rightarrow$ RS inconclusive.



RS verification for the gearbox

Termination Analysis

- Existence of an edge with weight $\infty \Rightarrow$ RS False.
- Existence of a cycle $\Rightarrow$ RS inconclusive.
- Existence of nodes with no outgoing edges different to the nodes on the boundary of the stability zone $\Rightarrow$ RS inconclusive.

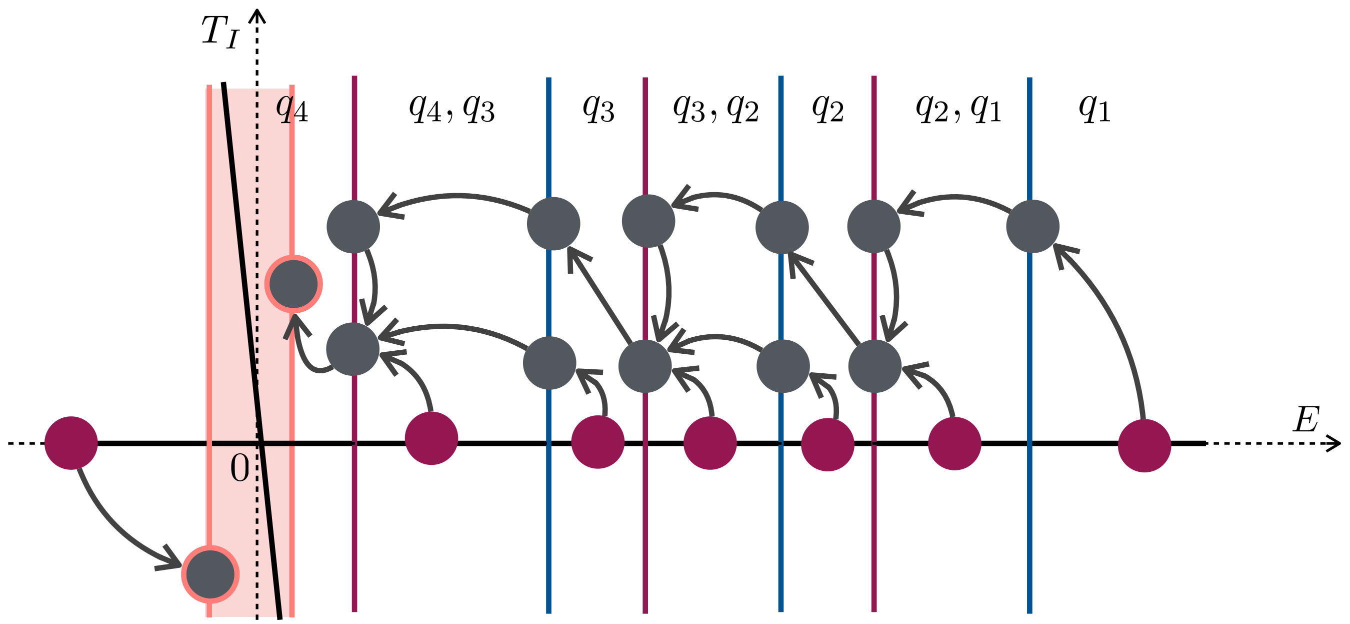


RS verification for the gearbox

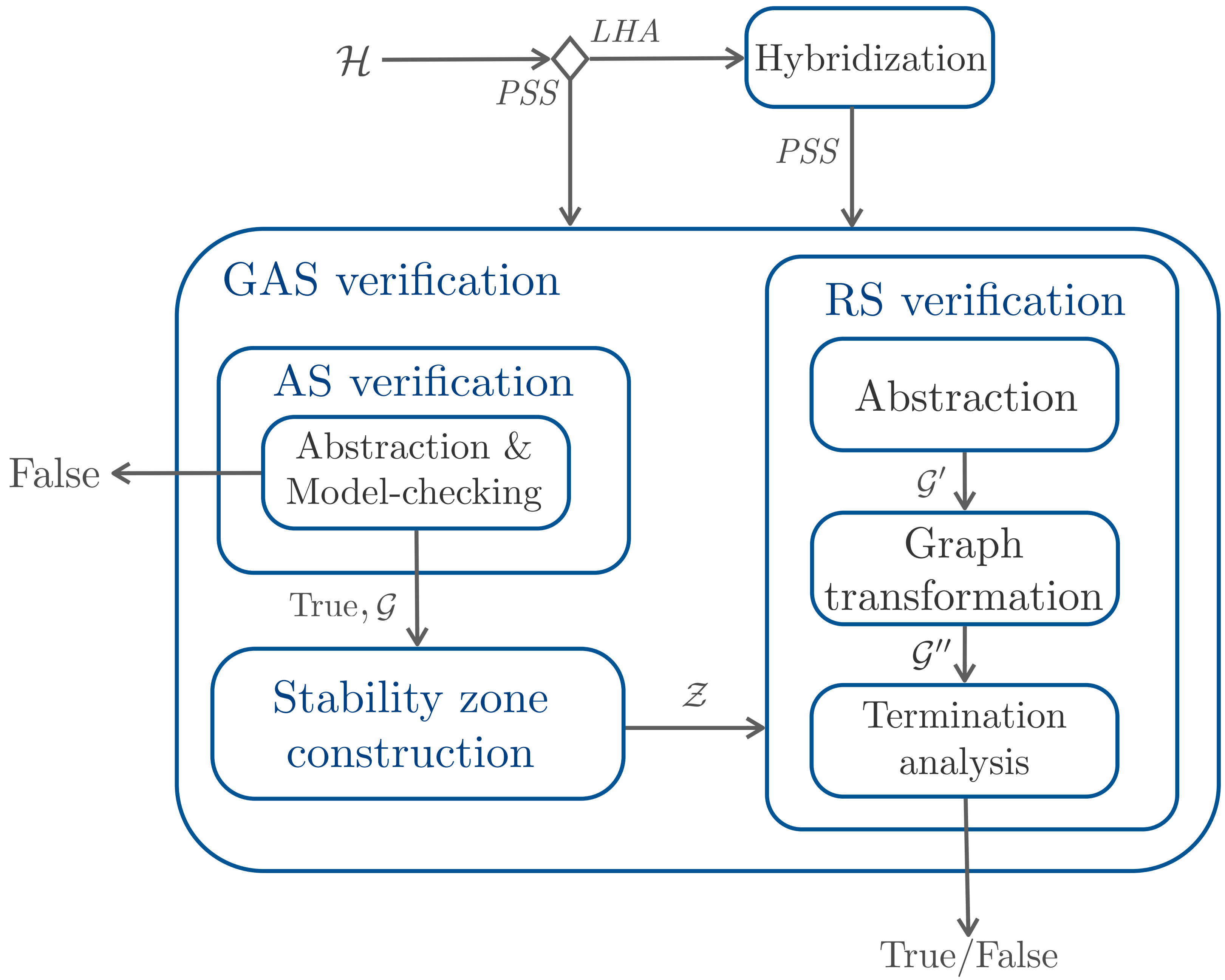
Termination Analysis

- Existence of an edge with weight $\infty \Rightarrow$ RS False.
- Existence of a cycle $\Rightarrow$ RS inconclusive.
- Existence of nodes with no outgoing edges different to the nodes on the boundary of the stability zone $\Rightarrow$ RS inconclusive.

Region stability established



Summary



$\mathcal{H}$
LHA
PSS
Hybridization
PSS
GAS verification
AS verification
Abstraction &
Model-checking
False
True, $\mathcal{G}$
Stability zone
construction
$\mathcal{Z}$
RS verification
Abstraction
$\mathcal{G}'$
Graph
transformation
$\mathcal{G}''$
Termination
analysis
True/False

Future research

- Extension of the algorithmic stability verification to non-linear systems.
- Compositional analysis for input-output stability verification.
- Synthesis of state based switching control for a family of dynamical systems.

Pavithra Prabhakar and Miriam García Soto, **Counterexample Guided Abstraction Refinement for Stability Analysis,** CAV 2016

———, **Hybridization for Stability Analysis of Switched Linear Systems,** HSCC 2016

———, **Foundations of Quantitative Predicate Abstraction for Stability Analysis of Hybrid Systems,** VMCAI 2015

———, **An algorithmic approach to stability verification of polyhedral switched systems,** ACC 2014

———, **Abstraction Based Model-Checking of Stability of Hybrid Systems,** CAV 2013

Thank you