The Image Computation Problem in Hybrid Systems Model Checking

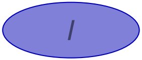
André Platzer[1,2] Edmund M. Clarke[2]

[1]University of Oldenburg, Department of Computing Science

[2]Carnegie Mellon University, Computer Science Department

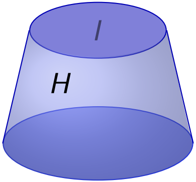
Hybrid Systems: Computation and Control (HSCC'2007)

Image Computation in Hybrid Systems



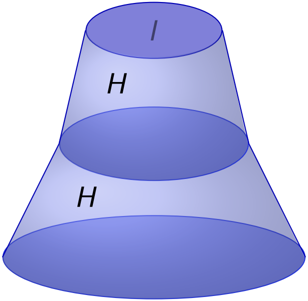
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



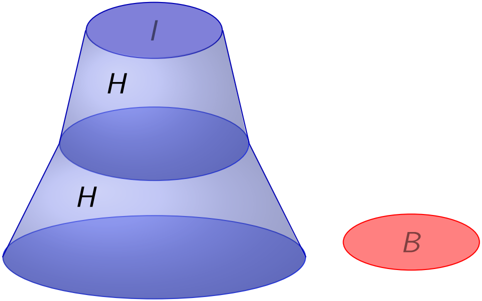
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



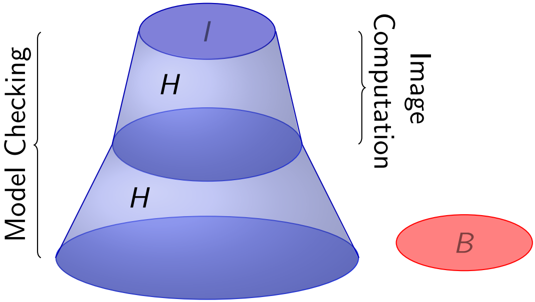
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems



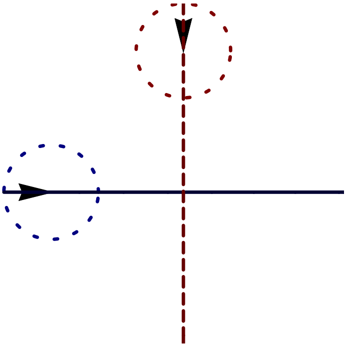
- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

Image Computation in Hybrid Systems

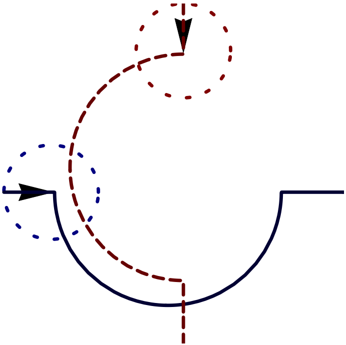


- Analyse image computation problem in hybrid systems
- Approximation refinement techniques and their limits

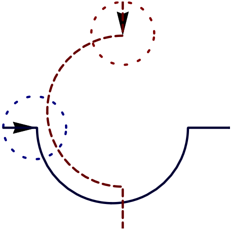
Air Traffic Management



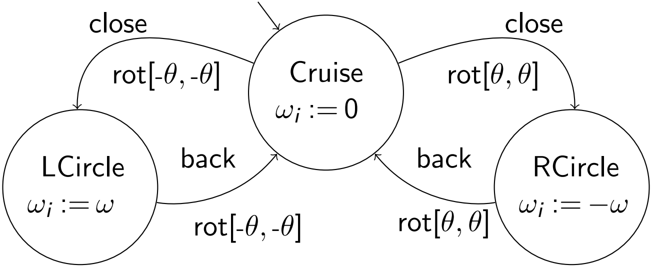
Air Traffic Management



ATM: Roundabout Maneuver Automaton



$$\begin{bmatrix} \dot{x} & = -v_1 & +v_2 \cos\phi & +\omega_1 y \\ \dot{y} & = & v_2 \sin\phi & -\omega_1 x \\ \dot{\phi} & = & \omega_2 & -\omega_1 \end{bmatrix}$$



Details

Outline

1. Motivation
   - Image Computation in Hybrid Systems
   - Air Traffic Management
2. Approximation in Model Checking
   - Approximation Refinement Model Checking
   - Exact Image Computation: Polynomials and Beyond
   - Image Approximation
3. Flow Approximation
   - Bounded Flow Approximation
   - Continuous Image Computation
   - Probabilistic Model Checking
   - Differential Flow Approximation
4. Experimental Results
5. Conclusions and Future Work

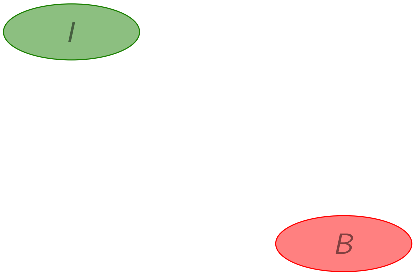
Outline

1. Motivation
   - Image Computation in Hybrid Systems
   - Air Traffic Management
2. Approximation in Model Checking
   - Approximation Refinement Model Checking
   - Exact Image Computation: Polynomials and Beyond
   - Image Approximation
3. Flow Approximation
   - Bounded Flow Approximation
   - Continuous Image Computation
   - Probabilistic Model Checking
   - Differential Flow Approximation
4. Experimental Results
5. Conclusions and Future Work

AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

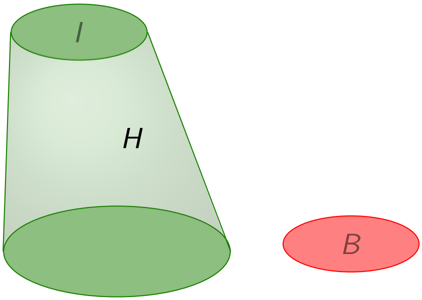
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

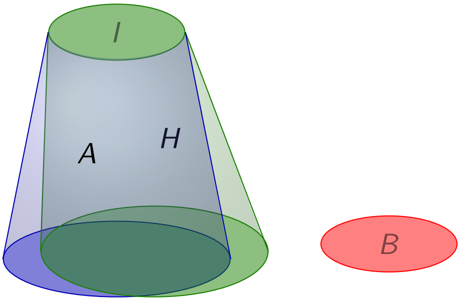
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

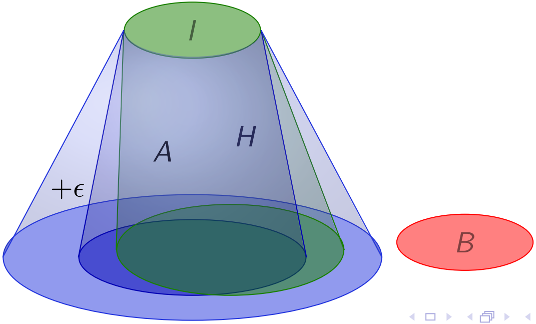
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

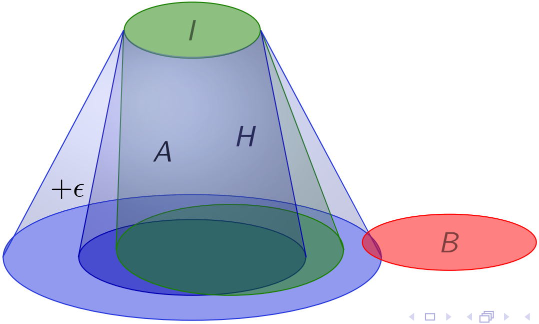
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

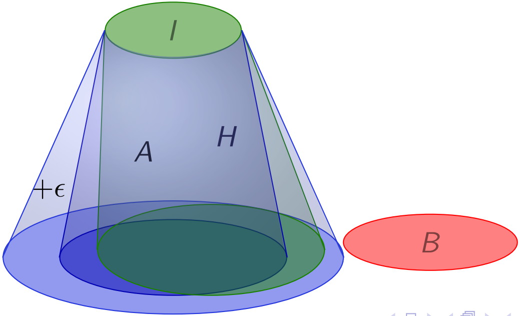
1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Approximation Refinement Model Checking

AMC(B reachable from I in H):

1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe



AMC: Exact Image Computation

AMC(B reachable from I in H):

1. $A := \text{approx}(H)$ uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe

Proposition

check and blur can be implemented for

- *I and B semialgebraic*
- *A with polynomial flows over* $\mathbf{R}$
- *+Piecewise definitions*
- *+Rational extensions (e.g. multivariate rational splines)*

AMC: Image Approximation

AMC(B reachable from I in H):

1. $A :=$ approx(H) uniformly
2. blur by uniform approximation error $+\epsilon$
3. check(B reachable from I in $A + \epsilon$)
4. B not reachable $\Rightarrow$ H safe

Proposition

approx exists for all uniform errors $\epsilon > 0$ when

- *using polynomials to build A*
- *Flows $\varphi \in C(D, \mathbf{R}^n)$ of H*
- *$D \subset \mathbf{R} \times \mathbf{R}^n$ compact closure of an open set*

Outline

1. Motivation
   - Image Computation in Hybrid Systems
   - Air Traffic Management
2. Approximation in Model Checking
   - Approximation Refinement Model Checking
   - Exact Image Computation: Polynomials and Beyond
   - Image Approximation
3. Flow Approximation
   - Bounded Flow Approximation
   - Continuous Image Computation
   - Probabilistic Model Checking
   - Differential Flow Approximation
4. Experimental Results
5. Conclusions and Future Work

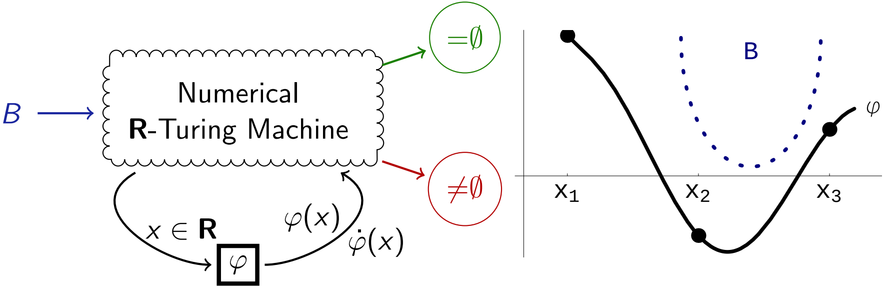
Bounded Flow Approximation

Proposition (Effective Weierstraß approximation)

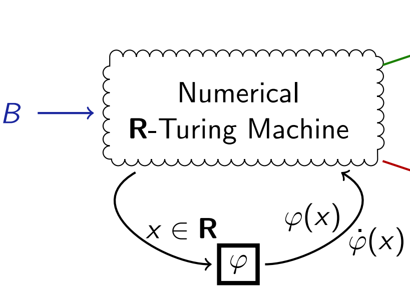
- *Flows* $\varphi \in C^1(D, \mathbf{R}^n)$
- *Bounds* $b := \max_{x \in D} \|\dot{\varphi}(x)\|$

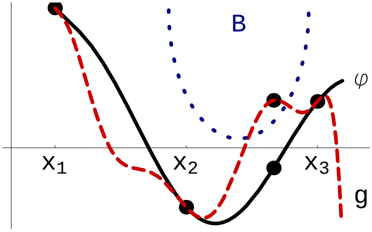
$\Rightarrow$ *approx computable, hence image computation decidable*

Continuous Image Computation

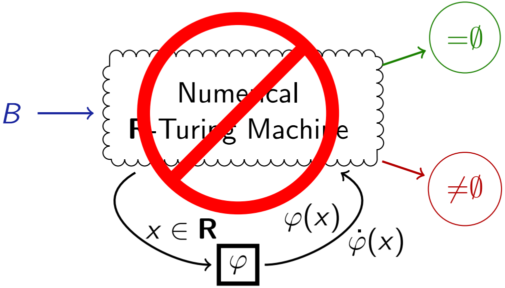


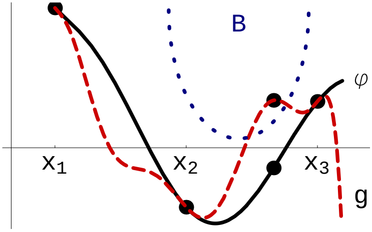
Continuous Image Computation





Continuous Image Computation

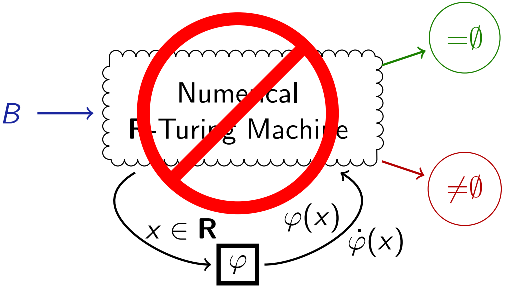


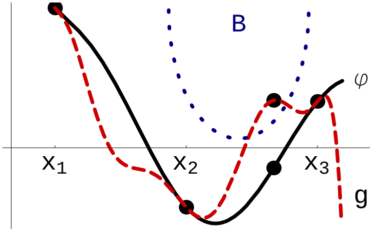


Proposition (Image computation undecidable for...)

- *arbitrarily effective flow* $\varphi \in C^k(D \subseteq \mathbf{R}^n, \mathbf{R}^m)$; *D, B effective*
- *tolerate error* $\epsilon > 0$ *in decisions*

Continuous Image Computation

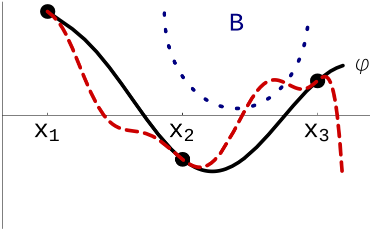




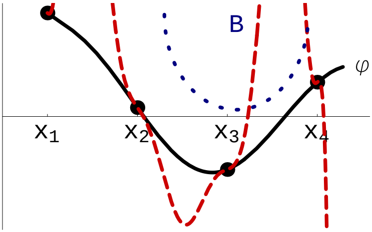
Proposition (Image computation undecidable for...)

- *arbitrarily effective flow* $\varphi \in C^k(D \subseteq \mathbf{R}^n, \mathbf{R}^m)$*; D, B effective*
- *tolerate error* $\epsilon > 0$ *in decisions*
- φ *smooth polynomial function with* $\mathbf{Q}$*-coefficients*

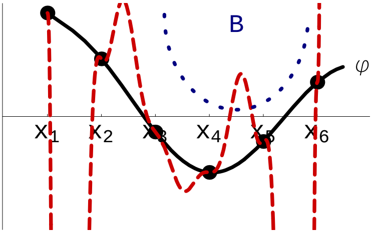
Probabilistic Model Checking



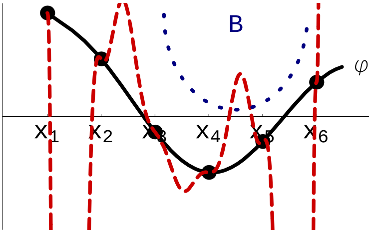
Probabilistic Model Checking



Probabilistic Model Checking



Probabilistic Model Checking

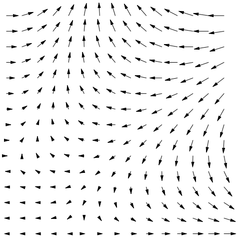


Proposition

- $P(\|\dot{\varphi}\|_\infty > b) \to 0$ *as* $b \to \infty$
- φ *evaluated on finite subset* $X = \{x_i\}$ *of open or compact* D

$\Rightarrow$ $P(\textit{decision correct}) \to 1$ *as* $\|d(\cdot, X)\|_\infty \to 0$

Differential Flow Approximation



φ solves
$\dot{x}(t) = f(t, x)$

Proposition

- *Flow φ is solution of $\dot{x}(t) = f(t, x)$*
- $f \in C([a, b] \times \mathbf{R}^n, \mathbf{R}^n)$
- *ℓ-Lipschitz-continuous:* $\|f(t, x_1) - f(t, x_2)\| \leq \ell \|x_1 - x_2\|$

$\Rightarrow$ *Continuous image computation decidable*

Outline

1 Motivation
- Image Computation in Hybrid Systems
- Air Traffic Management

2 Approximation in Model Checking
- Approximation Refinement Model Checking
- Exact Image Computation: Polynomials and Beyond
- Image Approximation

3 Flow Approximation
- Bounded Flow Approximation
- Continuous Image Computation
- Probabilistic Model Checking
- Differential Flow Approximation

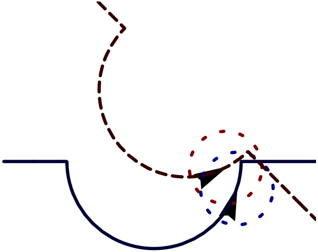
4 Experimental Results

5 Conclusions and Future Work

Experimental Results: Roundabout ATM

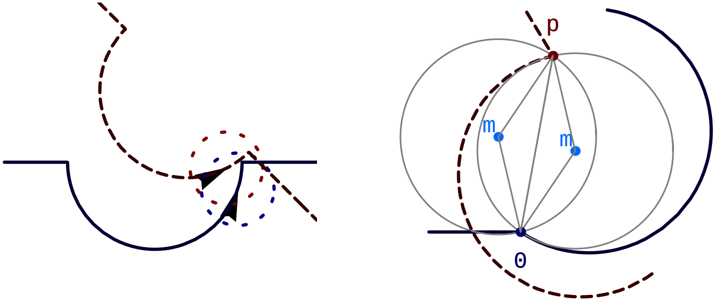
Counterexamples with distances ≈0.0016mi after 3 refinements

in absolute coords



Solution: adaptively choose rotation using tangential construction

classical | tangential



- ⊘ No more counterexamples
- Simple online calculation

Outline

1. Motivation
   - Image Computation in Hybrid Systems
   - Air Traffic Management
2. Approximation in Model Checking
   - Approximation Refinement Model Checking
   - Exact Image Computation: Polynomials and Beyond
   - Image Approximation
3. Flow Approximation
   - Bounded Flow Approximation
   - Continuous Image Computation
   - Probabilistic Model Checking
   - Differential Flow Approximation
4. Experimental Results
5. Conclusions and Future Work

Conclusions

- Image computation in hybrid systems model checking
  1. approx uniformly
  2. blur by uniform error
  3. check for B

flows	approx / image computation
continuous	uniform approx exists, but...
smooth	undecidable by evaluation
bounded by b	decidable
bound probabilities	probabilistically decidable
ODE ℓ-Lipschitz	decidable

- Combine numerical algorithms with symbolic analysis
- Roundabout maneuver unsafe
- Solution: adaptively choose rotations by tangential construction
- Report with details

Future Work

- Extend tangential roundabout maneuver
  - Determine speed/thrust bounds
  - Position discrepancies caused by imprecise tracking
  - Verify liveness: aircraft finally on original route
  - Full curve dynamics
- Combine numerical algorithms with symbolic analysis . . .
- Improve our preliminary model checker
- Multivariate rational spline approximation

Outline

6. Related Work

7. Details Air Traffic Management
   - Roundabout Maneuver Automaton
   - Adaptive Tangential Roundabout Maneuver

W. Damm, G. Pinto, and S. Ratschan.
Guaranteed termination in the verification of LTL properties of non-linear robust discrete time hybrid systems.
In *ATVA*, 2005.

R. Lanotte and S. Tini.
Taylor approximation for hybrid systems.
In *HSCC*, pages 402–416, 2005.

M. Massink and N. D. Francesco.
Modelling free flight with collision avoidance.
In *ICECCS*, pages 270–280, 2001.

C. Piazza, M. Antoniotti, V. Mysore, A. Policriti, F. Winkler, and B. Mishra.
Algorithmic algebraic model checking I.
In *CAV*, 2005.

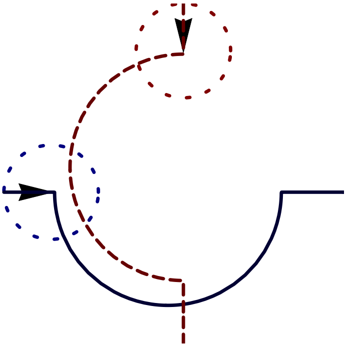
A. Platzer and E. M. Clarke.
The image computation problem in hybrid systems model checking.
Technical report, 2007.

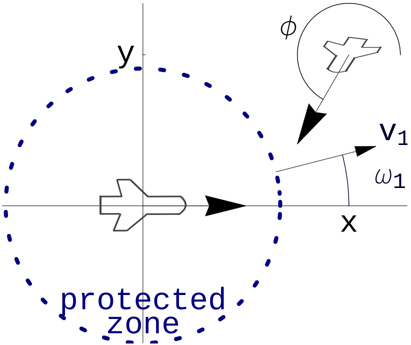
Outline

6 Related Work

7 Details Air Traffic Management
- Roundabout Maneuver Automaton
- Adaptive Tangential Roundabout Maneuver

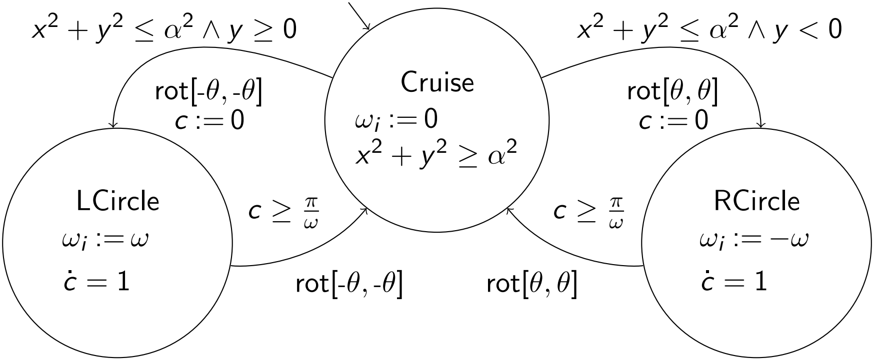
Air Traffic Management





ATM: Roundabout Maneuver Automaton

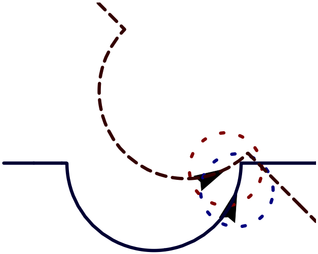
$$\begin{bmatrix} \dot{x} = -v_1 + v_2 \cos\phi + \omega_1 y \\ \dot{y} = v_2 \sin\phi - \omega_1 x \\ \dot{\phi} = \omega_2 - \omega_1 \end{bmatrix}$$



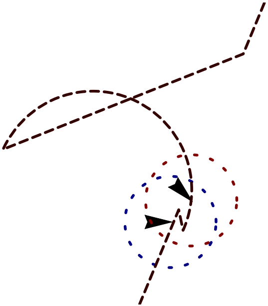
Return

- Counterexamples with distances ≈0.0016mi after 3 refinements

in absolute coords

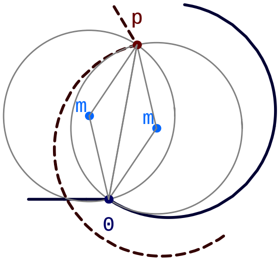


relative coords



Experimental Results: Tangential Roundabout ATM

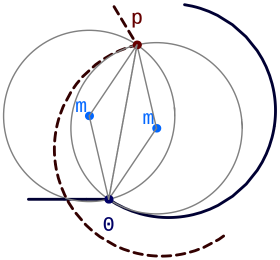
$$\alpha^2 = \|m - 0\|^2$$
$$\alpha^2 = \|m - p\|^2$$
$$\gamma_1 = \angle(m - 0)$$
$$\gamma_2 = \angle(m - p)$$



Return

Experimental Results: Tangential Roundabout ATM

$$\alpha^2 = \|m - 0\|^2$$
$$\alpha^2 = \|m - p\|^2$$
$$\gamma_1 = \angle(m - 0)$$
$$\gamma_2 = \angle(m - p)$$



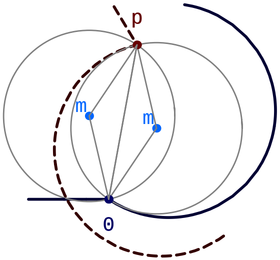
Solutions for θ_j using any $k, \ell \in \{1, 2\}$:

$$\angle\left((-1)^{j+1}\frac{x^3 + xy^2 + (-1)^{j+k}\imath\sqrt{x^2(x^2+y^2)(4\alpha^2 - x^2 - y^2)}}{x(x - \imath y)}\right) + (-1)^{\ell}\frac{\pi}{2}$$

Return

Experimental Results: Tangential Roundabout ATM

$$\alpha^2 = \|m - 0\|^2$$
$$\alpha^2 = \|m - p\|^2$$
$$\gamma_1 = \angle(m - 0)$$
$$\gamma_2 = \angle(m - p)$$



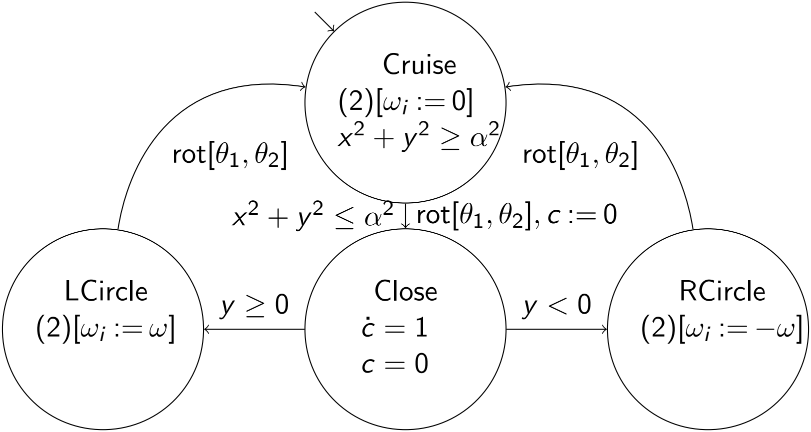
Solutions for θ_j using any $k, \ell \in \{1, 2\}$:

$$\angle\left((-1)^{j+1}\frac{x^3 + xy^2 + (-1)^{j+k}\imath\sqrt{x^2(x^2+y^2)(4\alpha^2 - x^2 - y^2)}}{x(x - \imath y)}\right) + (-1)^\ell\frac{\pi}{2}$$

$$\min_{k,\ell} \max(|\theta_1 - 0|, |\theta_2 - \phi|)$$

Return

Tangential Roundabout Maneuver Automaton



Return