

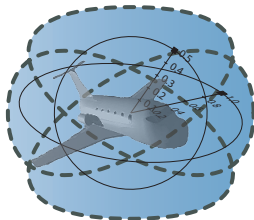
Formal Verification of Curved Flight Collision Avoidance Maneuvers

A Case Study

André Platzer Edmund M. Clarke

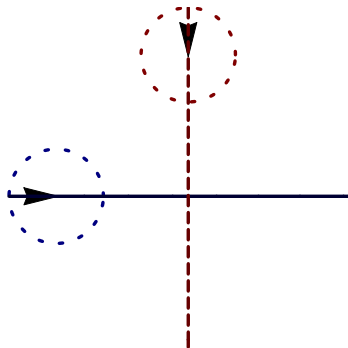
Carnegie Mellon University, Computer Science Department, Pittsburgh, PA

Formal Methods, FM, Eindhoven, November 2009

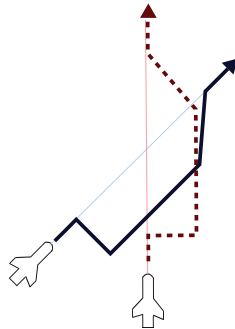
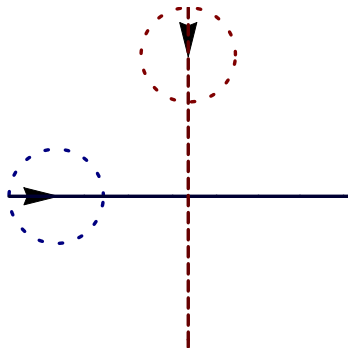


- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 Curved Flight Air Traffic Collision Avoidance Maneuver
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

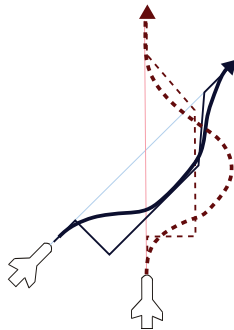
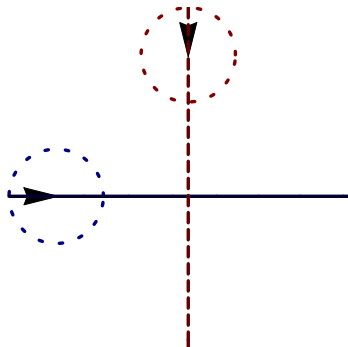
Ⓐ Air Traffic Control: Straight Lines & Instant Turns

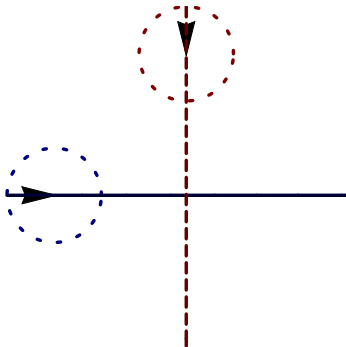


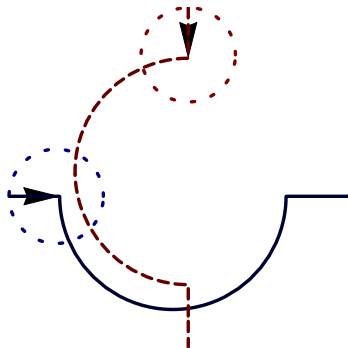
⌘ Air Traffic Control: Straight Lines & Instant Turns

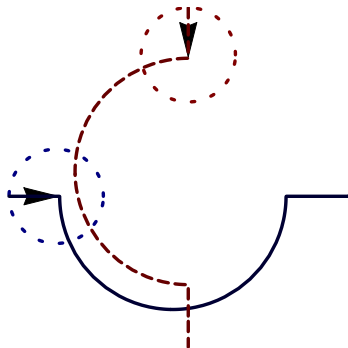


⌘ Air Traffic Control: Straight Lines & Instant Turns



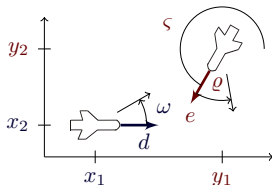
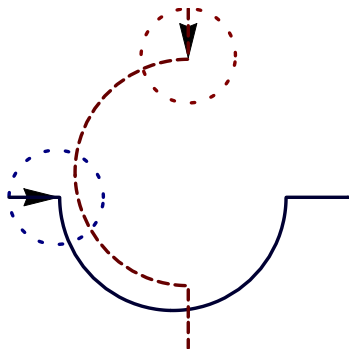






Hybrid Systems

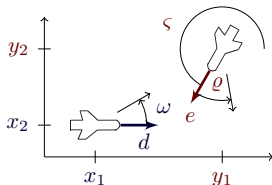
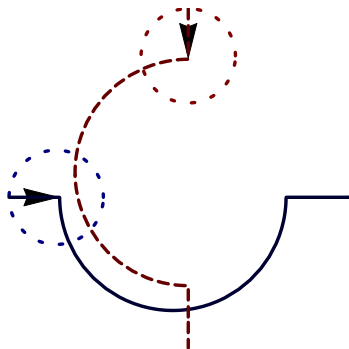
continuous evolution along differential equations + discrete change



$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos \vartheta + \omega x_2 \\ x_2' = v_2 \sin \vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{bmatrix}$$

Hybrid Systems

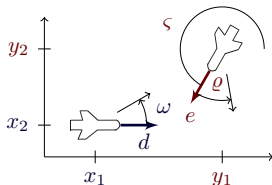
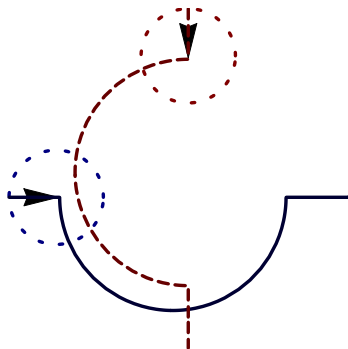
continuous evolution along differential equations + discrete change



$$\begin{cases} x_1' = -v_1 + v_2 \cos \vartheta + \omega x_2 \\ x_2' = v_2 \sin \vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{cases}$$

Example (“Solving” differential equations)

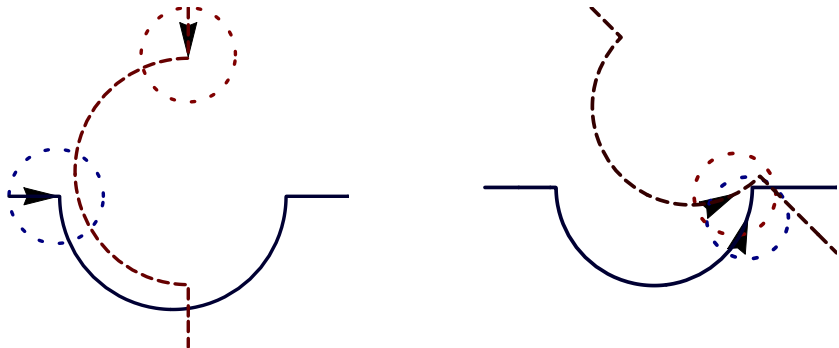
$$\begin{aligned} x_1(t) = & \frac{1}{\omega \varrho} (x_1 \omega \varrho \cos t\omega - v_2 \omega \cos t\omega \sin \vartheta + v_2 \omega \cos t\omega \cos t\varrho \sin \vartheta - v_1 \varrho \sin t\omega \\ & + x_2 \omega \varrho \sin t\omega - v_2 \omega \cos \vartheta \cos t\varrho \sin t\omega - v_2 \omega \sqrt{1 - \sin^2 \vartheta} \sin t\omega \\ & + v_2 \omega \cos \vartheta \cos t\omega \sin t\varrho + v_2 \omega \sin \vartheta \sin t\omega \sin t\varrho) \dots \end{aligned}$$



$$\begin{cases} x_1' = -v_1 + v_2 \cos \vartheta + \omega x_2 \\ x_2' = v_2 \sin \vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{cases}$$

Example (“Solving” differential equations)

$$\begin{aligned} \forall t \geq 0 \quad & \frac{1}{\omega \varrho} (x_1 \omega \varrho \cos t \omega - v_2 \omega \cos t \omega \sin \vartheta + v_2 \omega \cos t \omega \cos t \varrho \sin \vartheta - v_1 \varrho \sin t \omega \\ & + x_2 \omega \varrho \sin t \omega - v_2 \omega \cos \vartheta \cos t \varrho \sin t \omega - v_2 \omega \sqrt{1 - \sin^2 \vartheta} \sin t \omega \\ & + v_2 \omega \cos \vartheta \cos t \omega \sin t \varrho + v_2 \omega \sin \vartheta \sin t \omega \sin t \varrho) \dots \end{aligned}$$



Hybrid Systems

continuous evolution along differential equations + discrete change

Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems

Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)

Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
- Geometric intuition can be misleading

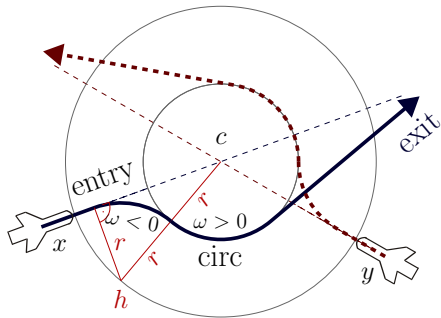
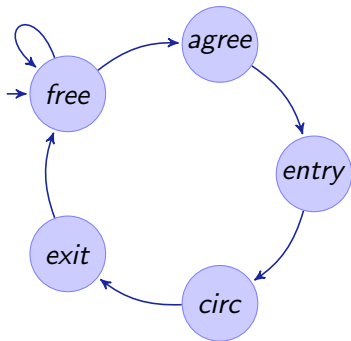
Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
- Geometric intuition can be misleading (\Rightarrow hybrid system model)

Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

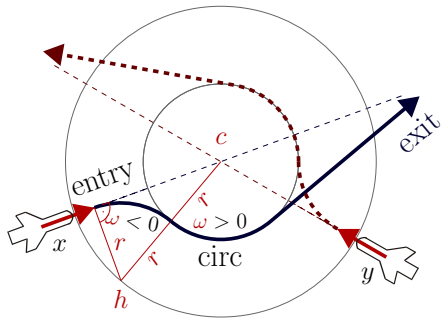
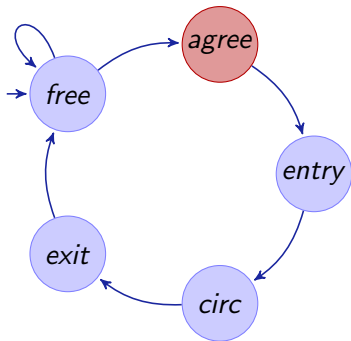
Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

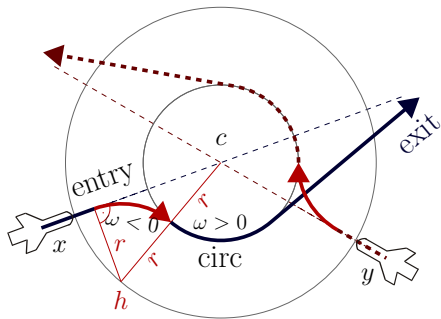
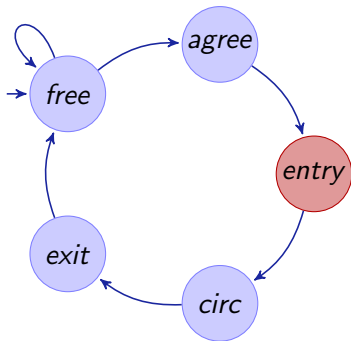
Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

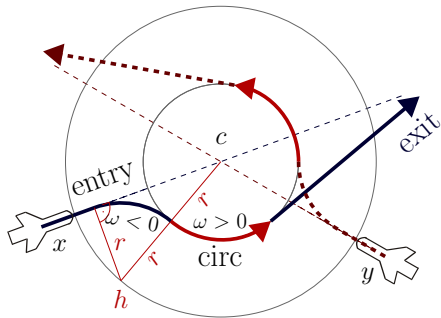
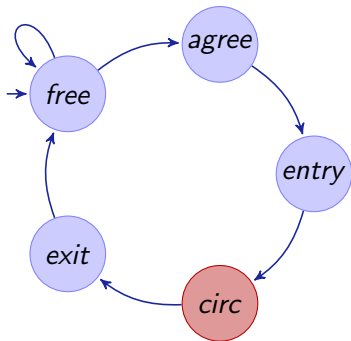
Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

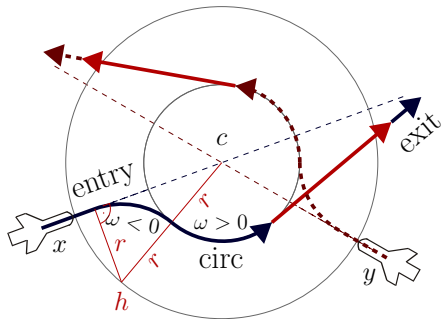
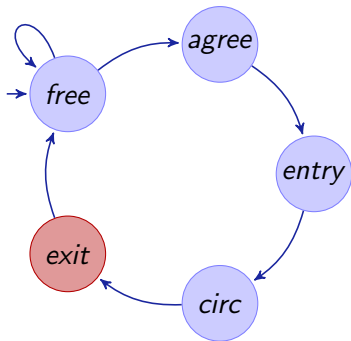
Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

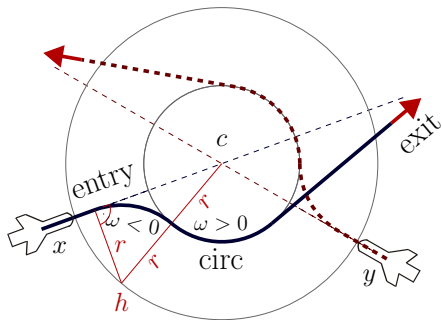
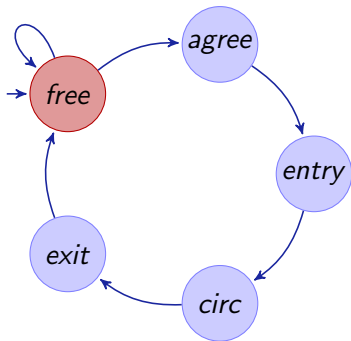
Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

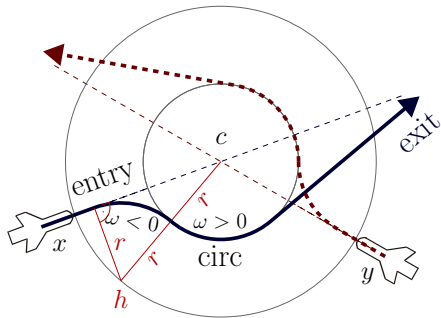
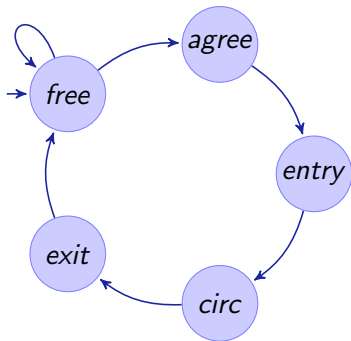
Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver



Problem \Rightarrow Solution

- Unrealistic instant turns can cause problems (\Rightarrow smooth curves)
 - Geometric intuition can be misleading (\Rightarrow hybrid system model)
- \Rightarrow Introduce smoothly curved flyable maneuver as hybrid system model

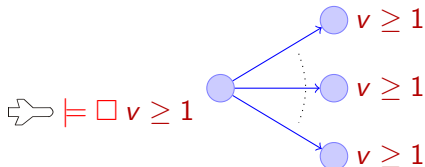
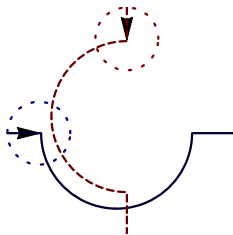
Verification for: nonlinear curve dynamics + mode switching?

- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 Curved Flight Air Traffic Collision Avoidance Maneuver
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 Curved Flight Air Traffic Collision Avoidance Maneuver
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

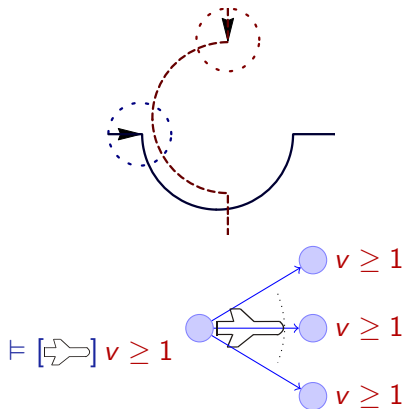
differential dynamic logic

$$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{ML}$$



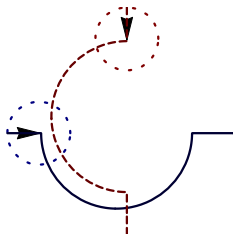
differential dynamic logic

$$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL}$$

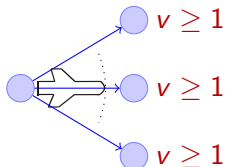


differential dynamic logic

$$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL} + \text{HP}$$

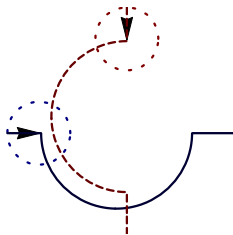


$$\models [d'_1 = -\omega d_2, d'_2 = \omega d_1] v \geq 1$$

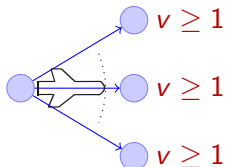


differential dynamic logic

$$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL} + \text{HP}$$

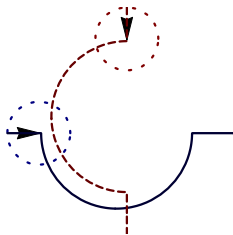


$$\models [\text{if}(x_1 > 0) \omega := 1; d'_1 = -\omega d_2, d'_2 = \omega d_1] v \geq 1$$

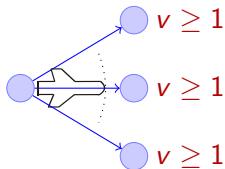


differential dynamic logic

$$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL} + \text{HP}$$



$$\models \underbrace{[\text{if}(x_1 > 0) \omega := 1; d'_1 = -\omega d_2, d'_2 = \omega d_1]}_{\text{hybrid program}} v \geq 1$$



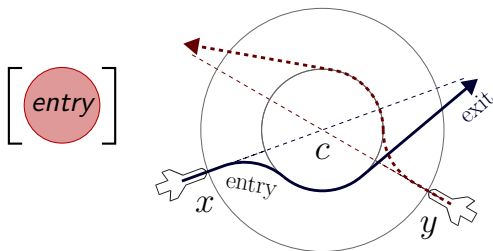
Definition (d \mathcal{L} Formula ϕ)

$\theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \rightarrow \psi \mid \forall x \phi \mid \exists x \phi \mid [\alpha]\phi \mid \langle \alpha \rangle \phi$

with terms θ_1, θ_2 of nonlinear real arithmetic $(+, \cdot)$

Definition (Hybrid program α)

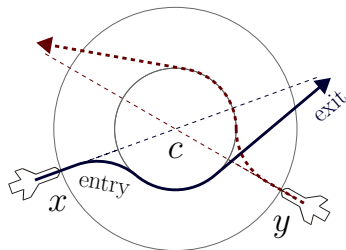
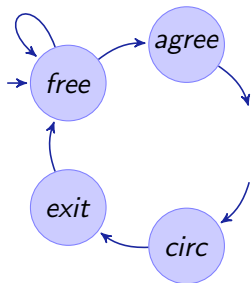
$x' = f(x) \wedge H$	(continuous evolution)	} jump & test
$x := f(x)$	(discrete jump)	
$?H$	(conditional execution)	
$\alpha; \beta$	(seq. composition)	
$\alpha \cup \beta$	(nondet. choice)	} Kleene algebra
α^*	(nondet. repetition)	



Example

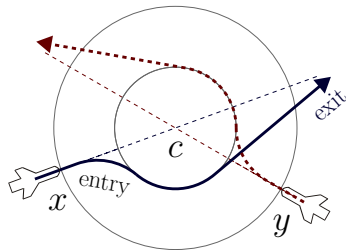
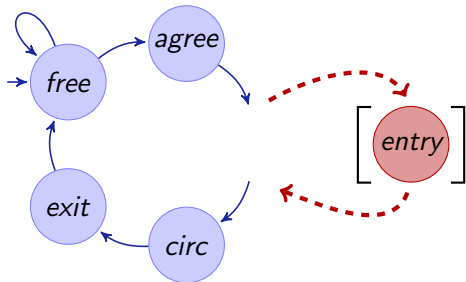
$$safe \wedge far \rightarrow [entry](safe \wedge tangential)$$

$$\text{where } safe \equiv (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



Example

$$\begin{aligned}
 \text{safe} \wedge \text{far} &\rightarrow [\text{entry}](\text{safe} \wedge \text{tangential}) \\
 \text{safe} \wedge \text{tangential} &\rightarrow [\text{other subsystem}]\text{safe} \\
 \text{where } \text{safe} &\equiv (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
 \end{aligned}$$

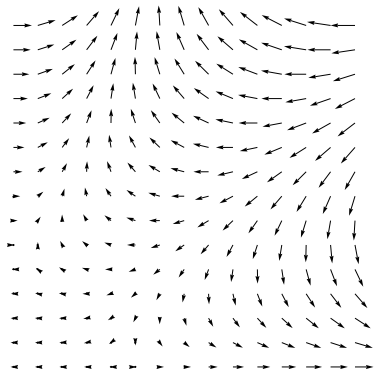


Example

$$\begin{array}{l}
 \text{safe} \wedge \text{far} \quad \rightarrow \quad [\text{entry}](\text{safe} \wedge \text{tangential}) \\
 \text{safe} \wedge \text{tangential} \quad \rightarrow \quad [\text{other subsystem}]\text{safe} \\
 \text{where } \text{safe} \quad \equiv \quad (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
 \end{array}
 \quad \left. \vphantom{\begin{array}{l} \text{safe} \wedge \text{far} \\ \text{safe} \wedge \text{tangential} \\ \text{where } \text{safe} \end{array}} \right\} \text{conjunction}$$

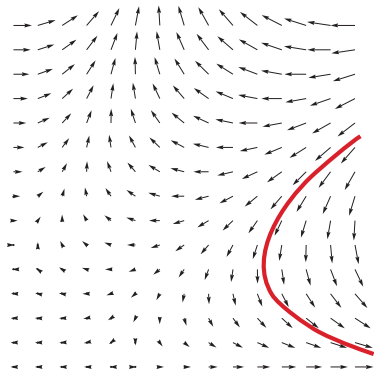
“Definition” (Differential Invariant)

“Formula that remains true in the direction of the dynamics”



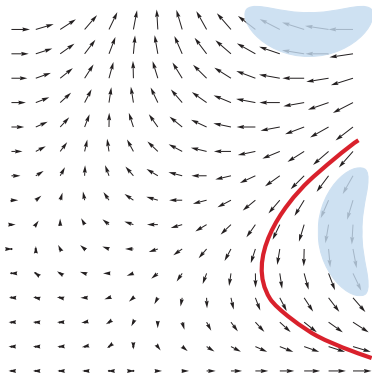
“Definition” (Differential Invariant)

“Formula that remains true in the direction of the dynamics”



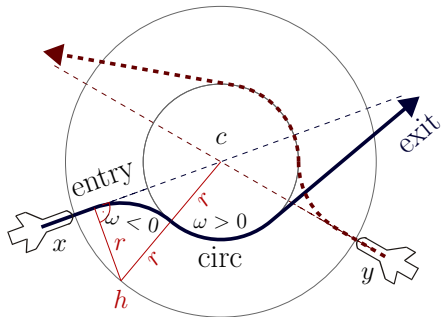
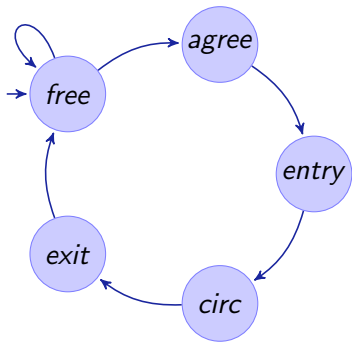
“Definition” (Differential Invariant)

“Formula that remains true in the direction of the dynamics”

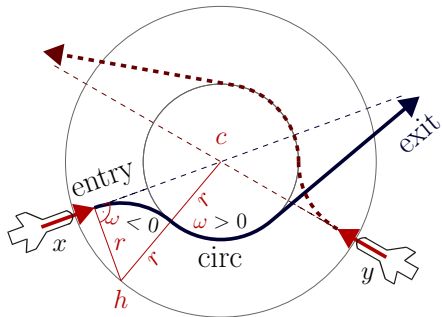
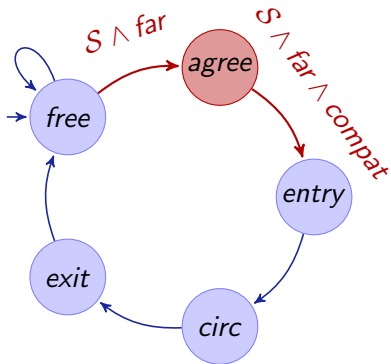


- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 **Curved Flight Air Traffic Collision Avoidance Maneuver**
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

Verification Loop for Air Traffic Control



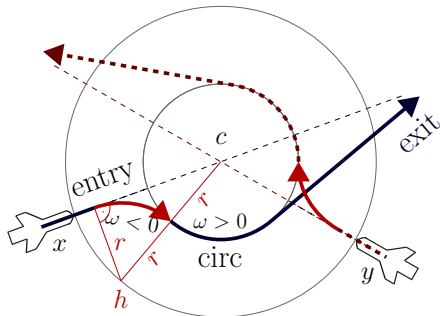
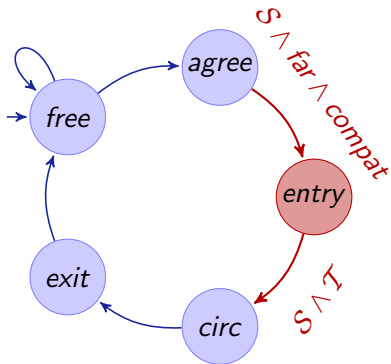
Verification Loop for Air Traffic Control



Example (d \mathcal{L} formula of verification subgoal)

$$safe \wedge far \rightarrow [agree](safe \wedge far \wedge compatible)$$

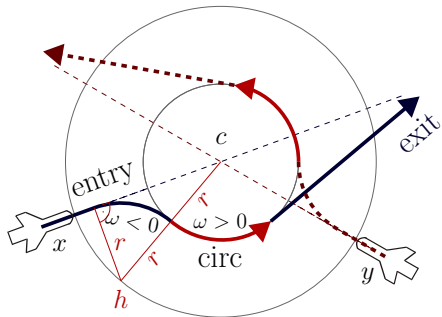
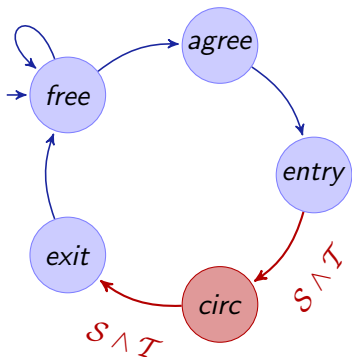
Verification Loop for Air Traffic Control



Example (d \mathcal{L} formula of verification subgoal)

$$safe \wedge far \wedge compatible \rightarrow [entry](safe \wedge tangential)$$

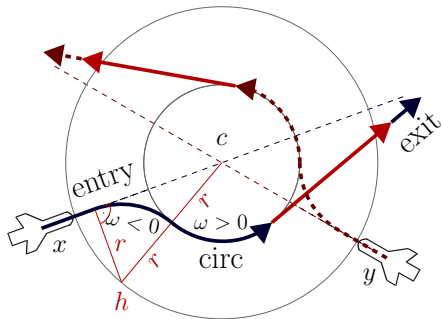
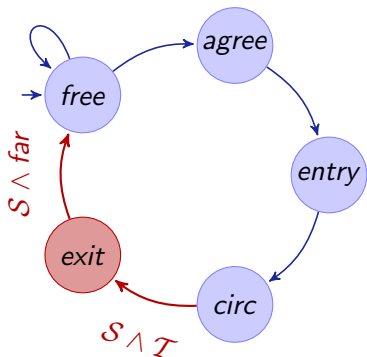
Verification Loop for Air Traffic Control



Example (d \mathcal{L} formula of verification subgoal)

$$safe \wedge tangential \rightarrow [circ](safe \wedge tangential)$$

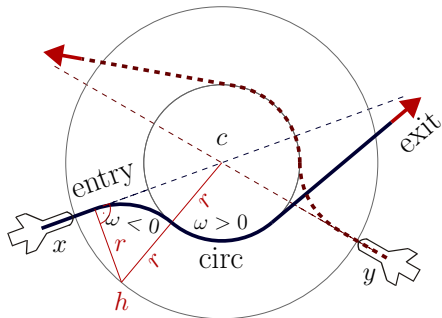
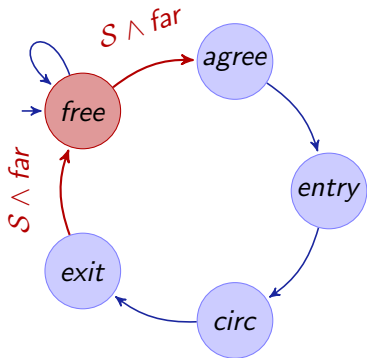
Verification Loop for Air Traffic Control



Example (d \mathcal{L} formula of verification subgoal)

$$safe \wedge tangential \rightarrow [exit](safe \wedge far)$$

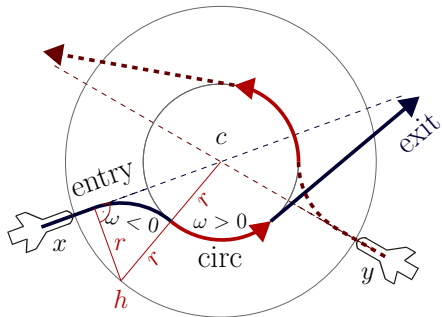
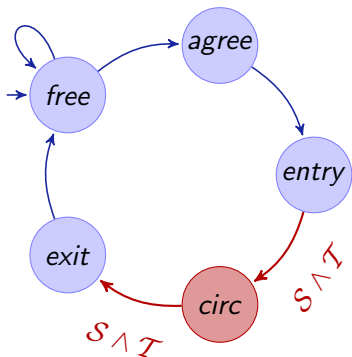
Verification Loop for Air Traffic Control



Example (d \mathcal{L} formula of verification subgoal)

$$safe \wedge far \rightarrow [free](safe \wedge far)$$

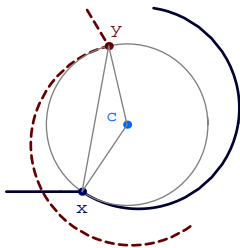
Verification Loop for Air Traffic Control



Example (d \mathcal{L} formula of verification subgoal)

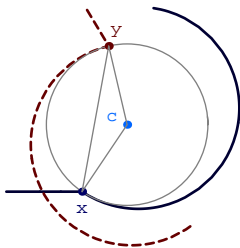
$$safe \wedge tangential \rightarrow [circ](safe \wedge tangential)$$

$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



Verify Roundabout Flight with Differential Invariants

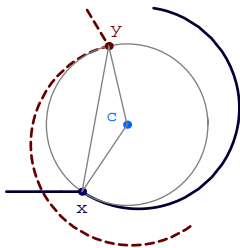
$$\frac{\partial \|x-y\|^2}{\partial x_1} x'_1 + \frac{\partial \|x-y\|^2}{\partial y_1} y'_1 + \frac{\partial \|x-y\|^2}{\partial x_2} x'_2 + \frac{\partial \|x-y\|^2}{\partial y_2} y'_2 \geq \frac{\partial p^2}{\partial x_1} x'_1 \dots$$
$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



Verify Roundabout Flight with Differential Invariants

$$\frac{\partial \|x-y\|^2}{\partial x_1} x'_1 + \frac{\partial \|x-y\|^2}{\partial y_1} y'_1 + \frac{\partial \|x-y\|^2}{\partial x_2} x'_2 + \frac{\partial \|x-y\|^2}{\partial y_2} y'_2 \geq \frac{\partial p^2}{\partial x_1} x'_1 \dots$$

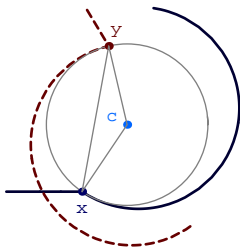
$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



Verify Roundabout Flight with Differential Invariants

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

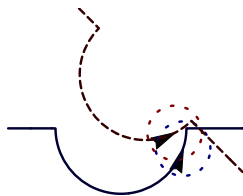
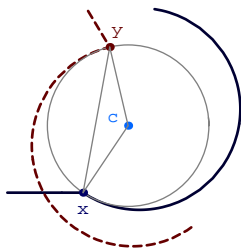


Verify Roundabout Flight with Differential Invariants

$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

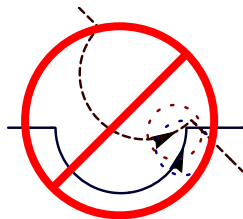
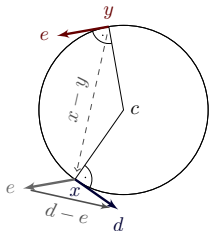


Verify Roundabout Flight with Differential Invariants

$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



$$[d'_1 = -\omega d_2, e'_1 = -\omega e_2, x'_2 = d_2, d'_2 = \omega d_1 \dots] d_1 - e_1 = -\omega(x_2 - y_2)$$

$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

Proposition (Differential saturation)

F differential invariant of $[x' = \theta \wedge H]S$, then
 $[x' = \theta \wedge H]S$ iff $[x' = \theta \wedge H \wedge F]S$

$$[d'_1 = -\omega d_2, e'_1 = -\omega e_2, x'_2 = d_2, d'_2 = \omega d_1 \dots] d_1 - e_1 = -\omega(x_2 - y_2)$$

Verify Roundabout Flight with Differential Invariants

$$2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

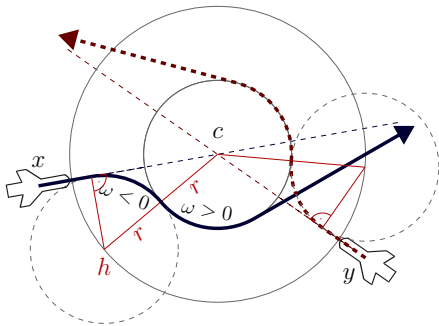
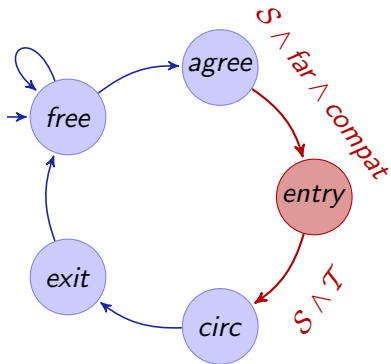
$$[x'_1 = d_1, d'_1 = -\omega d_2, x'_2 = d_2, d'_2 = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

Proposition (Differential saturation)

F differential invariant of $[x' = \theta \wedge H]S$, then
 $[x' = \theta \wedge H]S$ iff $[x' = \theta \wedge H \wedge F]S$

$$[d'_1 = -\omega d_2, e'_1 = -\omega e_2, x'_2 = d_2, d'_2 = \omega d_1 \dots] d_1 - e_1 = -\omega(x_2 - y_2)$$

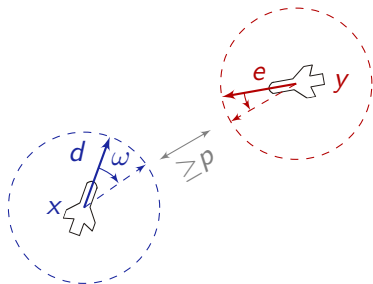
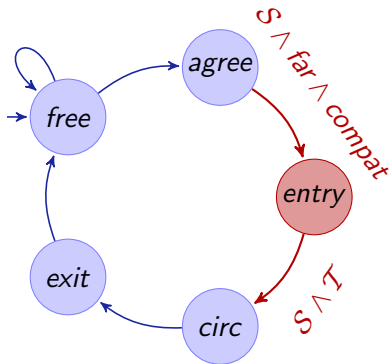
Flyable Roundabout Maneuver: Entry



Example (d \mathcal{L} formula of verification subgoal: reach tangential)

$$\begin{aligned}
 (r\omega)^2 &= \|d\|^2 \wedge \|x - c\| = \sqrt{3}r \wedge \exists \lambda \geq 0 (x + \lambda d = c) \wedge \\
 &\quad \|h - c\| = 2r \wedge d = -\omega(x - h)^\perp \\
 &\rightarrow [\mathcal{F}(-\omega) \wedge \|x - c\| \geq r] (\|x - c\| \leq r \rightarrow d = \omega(x - c)^\perp)
 \end{aligned}$$

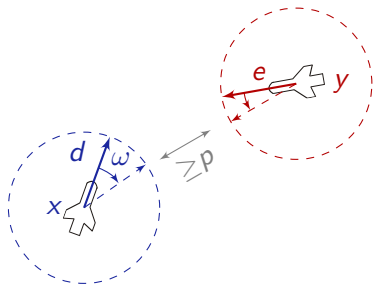
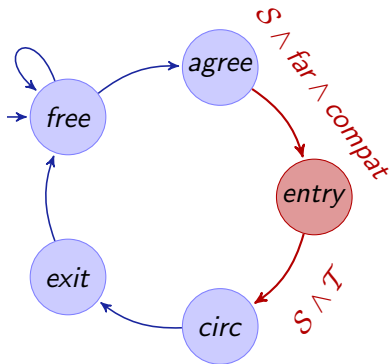
Flyable Roundabout Maneuver: Entry



Example (d \mathcal{L} formula of verification subgoal: stay separate)

$$\|x - y\| \geq \sqrt{2}(p + 2bT) \wedge p \geq 0 \wedge \|d\|^2 \leq \|e\|^2 \leq b^2 \wedge b \geq 0 \wedge T \geq 0$$

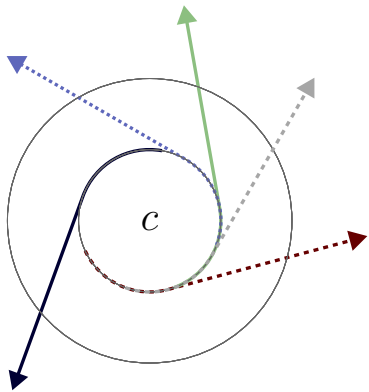
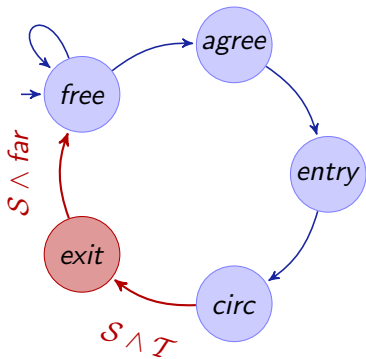
$$\rightarrow [\text{entry}] (\|x - y\| \geq p)$$



Example (dL formula of verification subgoal: limited progress)

$$x = z \wedge \|d\|^2 \leq b^2 \wedge b \geq 0$$

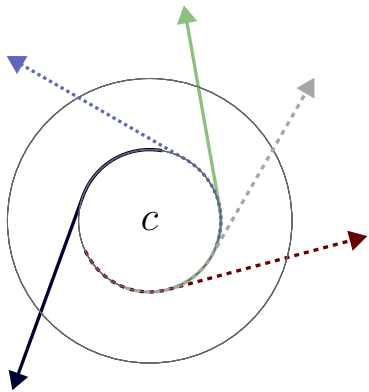
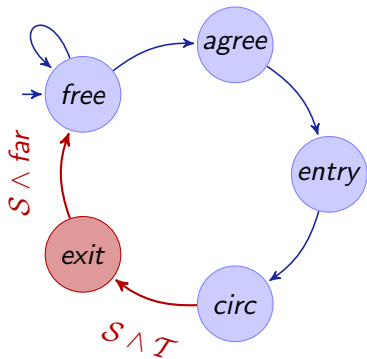
$$\rightarrow [\tau := 0; \exists \omega \mathcal{F}(\omega) \wedge \tau' = 1] (\|x - z\|_\infty \leq \tau b)$$



Example (d \mathcal{L} formula of verification subgoal: separated exit)

$$\mathcal{T} \wedge \|x - y\|^2 \geq p^2 \rightarrow [x' = d \wedge y' = e] (\|x - y\|^2 \geq p^2)$$

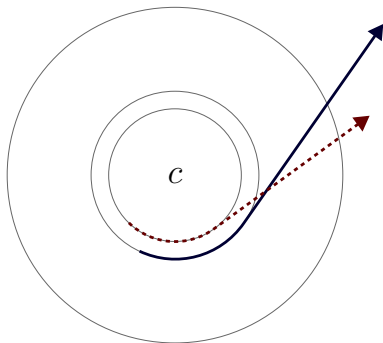
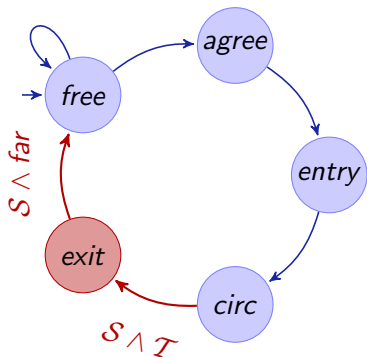
Flyable Roundabout Maneuver: Exit



Example (d \mathcal{L} formula of verification subgoal: separate directions)

$$\mathcal{T} \wedge \|x - y\|^2 \geq p^2 \rightarrow [x' = d; y' = e] (\|x - y\|^2 \geq p^2)$$

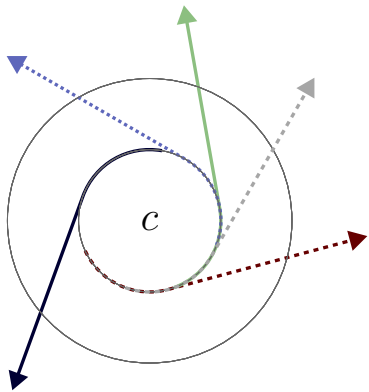
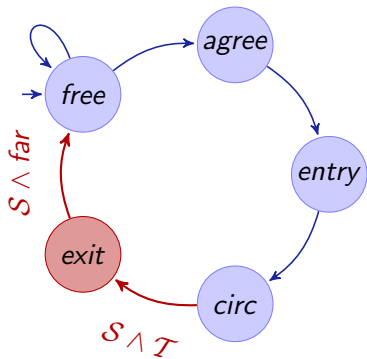
Flyable Roundabout Maneuver: Exit



Example (d \mathcal{L} formula of verification subgoal: separate directions)

$$\mathcal{T} \wedge \|x - y\|^2 \geq p^2 \rightarrow [x' = d; y' = e] (\|x - y\|^2 \geq p^2)$$

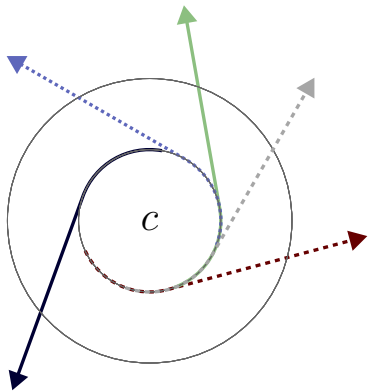
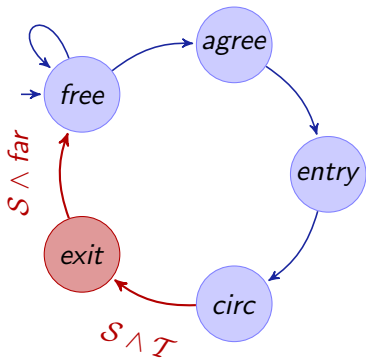
Flyable Roundabout Maneuver: Exit



Example ($d\mathcal{L}$ formula of verification subgoal: separate directions)

$$\mathcal{T} \wedge \|x - y\|^2 \geq p^2 \rightarrow [x' = d; y' = e] (\|x - y\|^2 \geq p^2)$$

Flyable Roundabout Maneuver: Exit

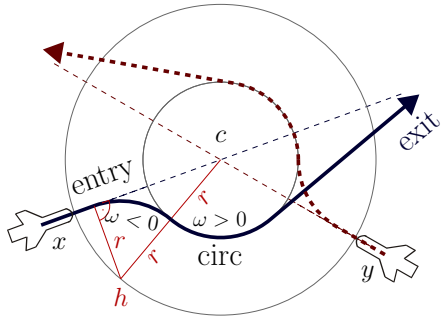
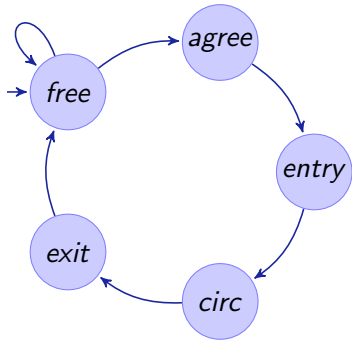


Example (d \mathcal{L} formula of verification subgoal: far separability)

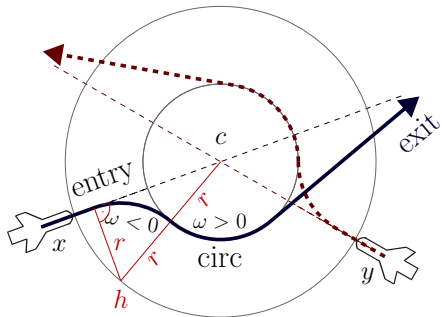
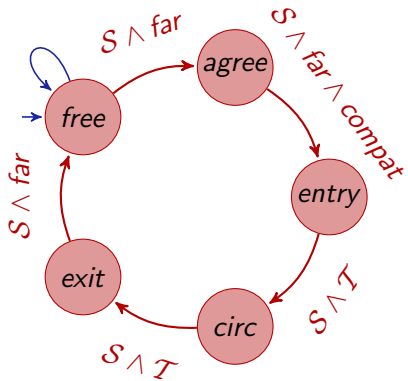
$$\mathcal{T} \wedge d \neq e \rightarrow \forall a \langle x' = d \wedge y' = e \rangle (\|x - y\|^2 > a^2)$$

- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 Curved Flight Air Traffic Collision Avoidance Maneuver
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

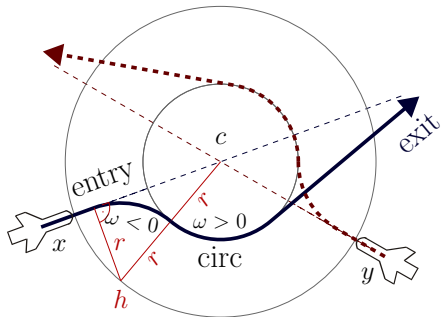
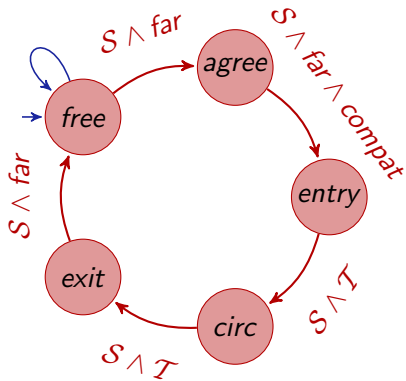
Flyable Roundabout Maneuver: Summary



⌘ Flyable Roundabout Maneuver: Summary



Flyable Roundabout Maneuver: Summary



Theorem (Collision freedom)

FTRM is collision free:

$$\|x - y\| \geq \text{far} \wedge \dots \rightarrow [\text{FTRM}] \|x - y\| \geq p$$

- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 Curved Flight Air Traffic Collision Avoidance Maneuver
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

Experimental Results

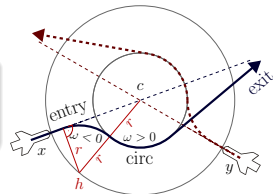
Case Study	Time(s)	Mem(Mb)	Steps	Dim
tangential roundabout (2a/c)	10.4	6.8	197	13
tangential roundabout (3a/c)	253.6	7.2	342	18
tangential roundabout (4a/c)	382.9	10.2	520	23
tangential roundabout (5a/c)	1882.9	39.1	735	28
bounded maneuver speed	0.5	6.3	14	4
flyable roundabout entry*	10.1	9.6	132	8
flyable entry feasible*	104.5	87.9	16	10
flyable entry circular	3.2	7.6	81	5
limited entry progress	1.9	6.5	60	8
entry separation	140.1	20.1	512	16
mutual negotiation successful	0.8	6.4	60	12
mutual negotiation feasible*	7.5	23.8	21	11
mutual far negotiation	2.4	8.1	67	14
simultaneous exit separation*	4.3	12.9	44	9
different exit directions	3.1	11.1	42	11

- 1 Motivation
- 2 Differential Dynamic Logic for Hybrid Systems
 - Compositional Verification Logic
 - Differential Invariants
- 3 Curved Flight Air Traffic Collision Avoidance Maneuver
 - Compositional Verification Plan
 - Verifying Roundabout Flight
 - Safe Flyable Entry Separation
 - Safe Exit Separation
 - Successful Negotiation & Synchronization
- 4 Flyable Tangential Roundabout Maneuver
- 4 Experimental Results
- 5 Conclusions & Future Work

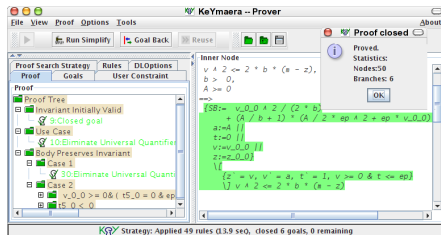
- Scaling verification technology
- Scaling air traffic control scenarios
- Relax remaining modeling assumptions (e.g., synch)
Proof structure is general but computational complexity challenging
- Develop and verify other entry procedure, maneuver choices, ...

differential dynamic logic

$$d\mathcal{L} = DL + HP$$



- Real aircraft follow smooth curves
- Geometric intuition may mislead
- Flyable Roundabout Maneuver
- Verification in logic $d\mathcal{L}$
- Differential invariants instead of reachability along solutions
- **Formal verification can scale to real aircraft maneuvers!**



KeYmaera