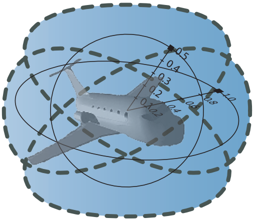
Differential Invariants for Collision Avoidance

André Platzer   Edmund M. Clarke

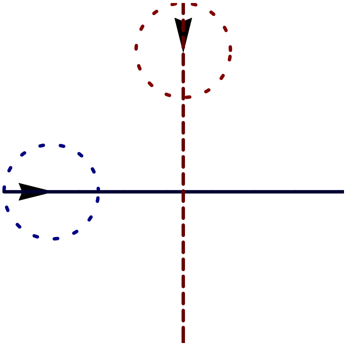
Carnegie Mellon University, Computer Science Department, Pittsburgh, PA

NSF CMACS Expedition

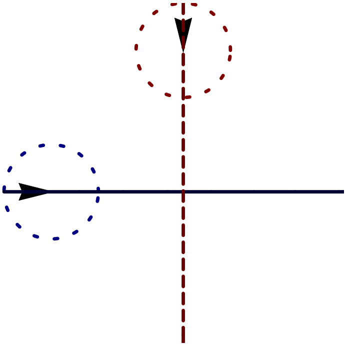


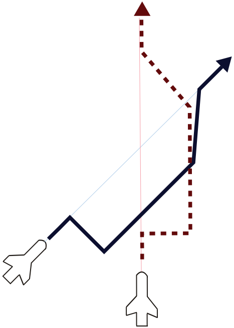
Outline

Air Traffic Control: Straight Lines & Instant Turns

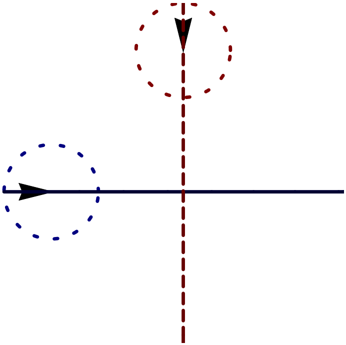


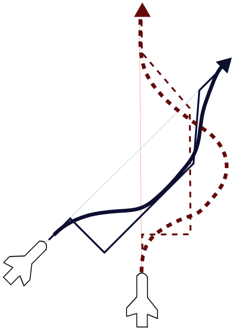
Air Traffic Control: Straight Lines & Instant Turns



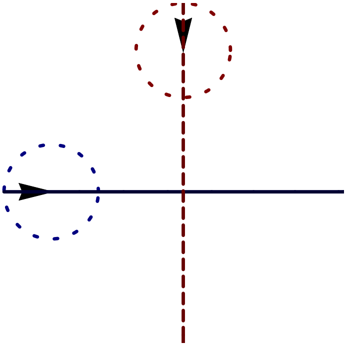


Air Traffic Control: Straight Lines & Instant Turns

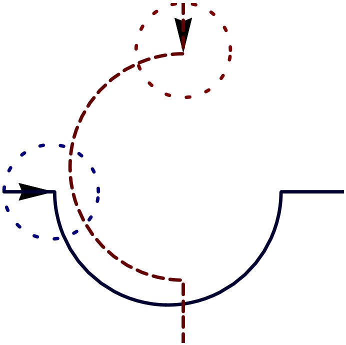




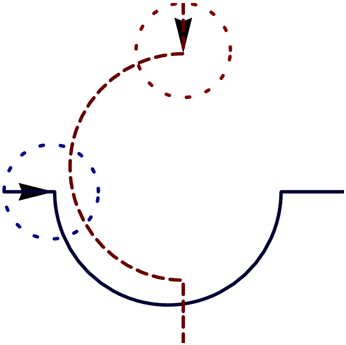
Air Traffic Control: Hybrid Systems & Curves



Air Traffic Control: Hybrid Systems & Curves

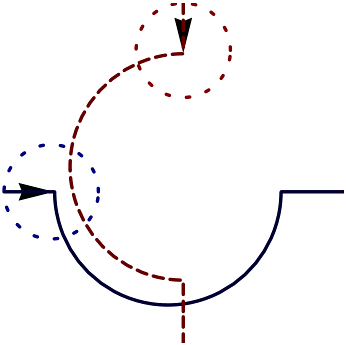


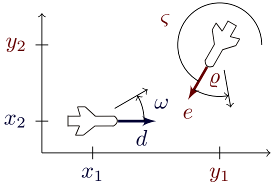
Air Traffic Control: Hybrid Systems & Curves



Hybrid Systems

continuous evolution along differential equations + discrete change

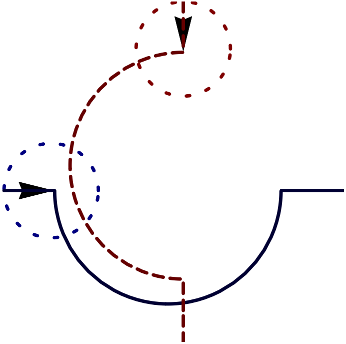


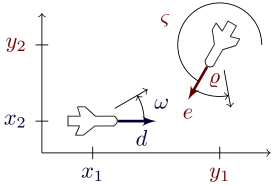


$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{bmatrix}$$

Hybrid Systems

continuous evolution along differential equations + discrete change



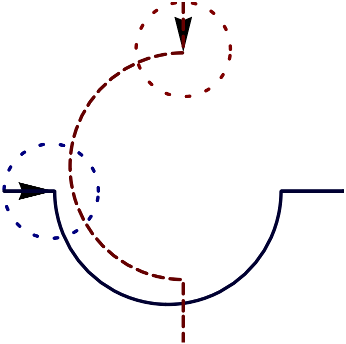


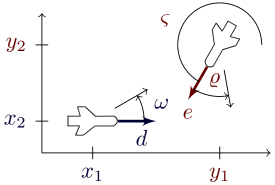
$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$$x_1(t) = \frac{1}{\omega\varrho}\big(x_1\omega\varrho\cos t\omega - v_2\omega\cos t\omega\sin\vartheta + v_2\omega\cos t\omega\cos t\varrho\sin\vartheta - v_1\varrho\sin t\omega$$
$$+ x_2\omega\varrho\sin t\omega - v_2\omega\cos\vartheta\cos t\varrho\sin t\omega - v_2\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$$
$$+ v_2\omega\cos\vartheta\cos t\omega\sin t\varrho + v_2\omega\sin\vartheta\sin t\omega\sin t\varrho\big)\ldots$$

Air Traffic Control: Hybrid Systems & Curves





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

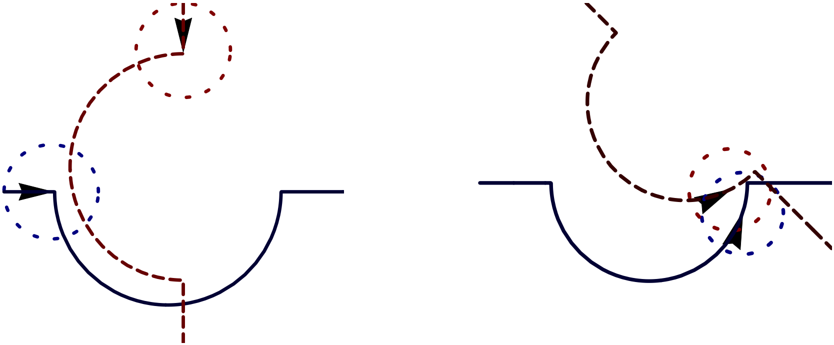
Example ("Solving" differential equations)

$$\forall t \geq 0 \quad \frac{1}{\omega\varrho}\Big(x_1\omega\varrho\cos t\omega - v_2\omega\cos t\omega\sin\vartheta + v_2\omega\cos t\omega\cos t\varrho\sin\vartheta - v_1\varrho\sin t\omega$$

$$+ x_2\omega\varrho\sin t\omega - v_2\omega\cos\vartheta\cos t\varrho\sin t\omega - v_2\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$$

$$+ v_2\omega\cos\vartheta\cos t\omega\sin t\varrho + v_2\omega\sin\vartheta\sin t\omega\sin t\varrho\Big)\ldots$$

Air Traffic Control: Hybrid Systems & Curves



Hybrid Systems

continuous evolution along differential equations + discrete change

Introduce: Flyable Roundabout Maneuver

Problem ⇒ Solution

- Unrealistic instant turns can cause problems

Introduce: Flyable Roundabout Maneuver

Problem $\Rightarrow$ Solution

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

Introduce: Flyable Roundabout Maneuver

Problem $\Rightarrow$ Solution

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

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)

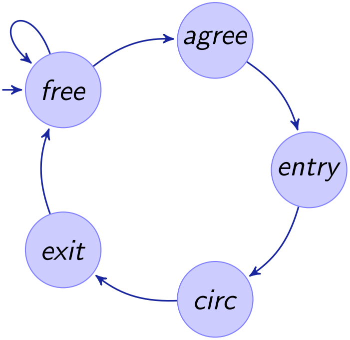
Introduce: Flyable Roundabout Maneuver

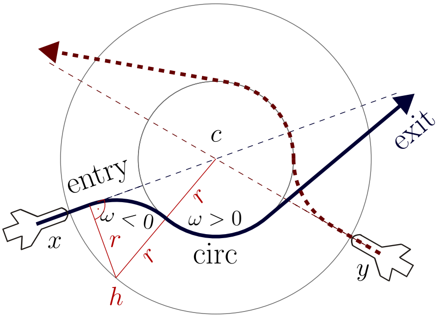
Problem $\Rightarrow$ Solution

- 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



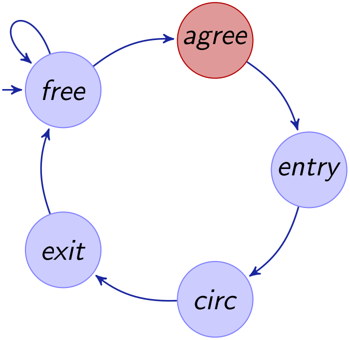


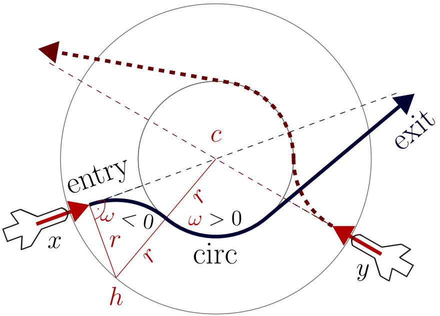
Problem ⇒ Solution

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

⇒ Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver



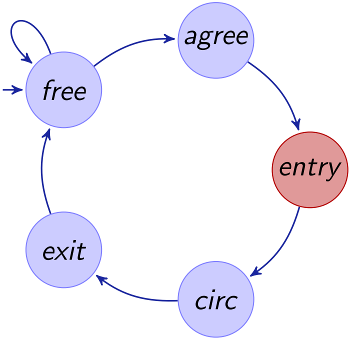


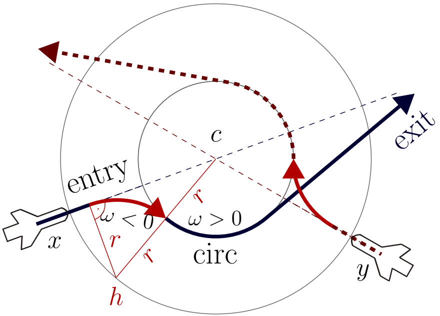
Problem ⇒ Solution

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

⇒ Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver



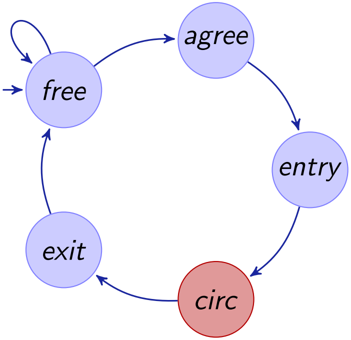


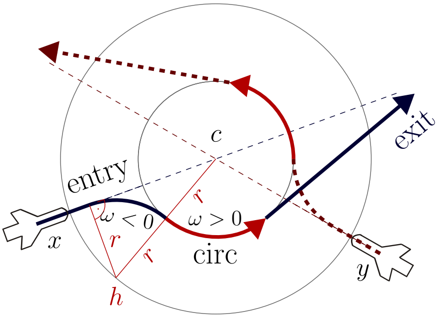
Problem ⇒ Solution

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

⇒ Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver



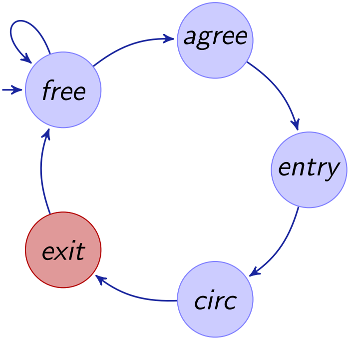


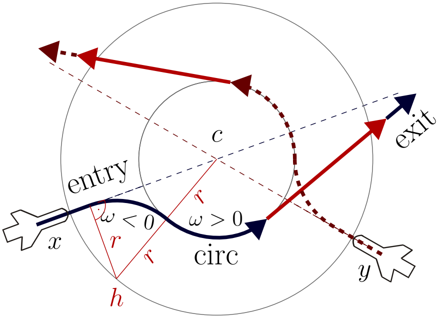
Problem ⇒ Solution

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

⇒ Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver



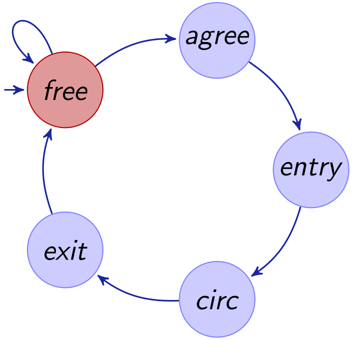


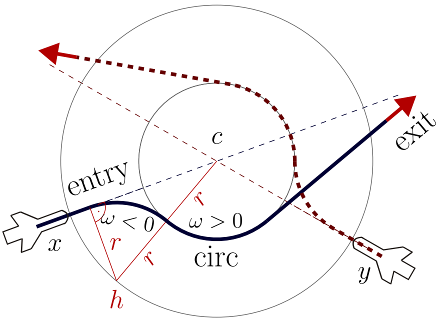
Problem ⇒ Solution

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

⇒ Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver



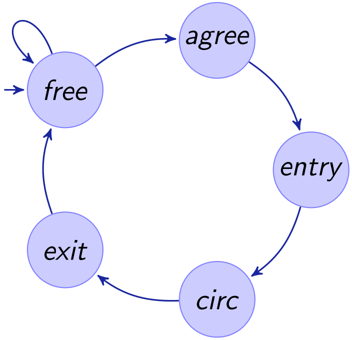


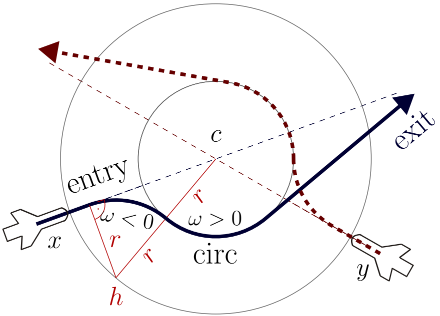
Problem ⇒ Solution

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

⇒ Introduce smoothly curved flyable maneuver as hybrid system model

Introduce: Flyable Roundabout Maneuver





Problem $\Rightarrow$ Solution

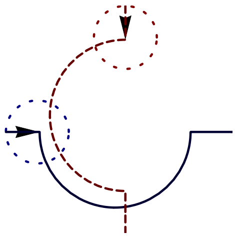
- Unrealistic instant turns can cause problems ($\Rightarrow$ smooth curves)
- Geometric intuition can be misleading ($\Rightarrow$ hybrid system model)

$\Rightarrow$ Introduce smoothly curved flyable maneuver as hybrid system model

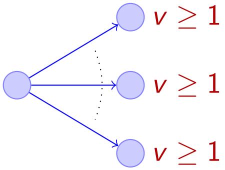
Verification for: nonlinear curve dynamics + mode switching?

Outline

Outline

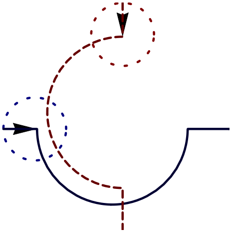


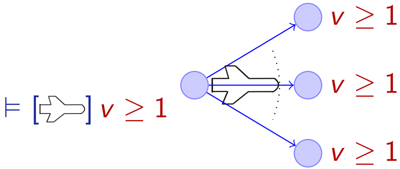
$\models \Box\, v \geq 1$



differential dynamic logic

$d\mathcal{L} = FOL_{\mathbb{R}} + DL$

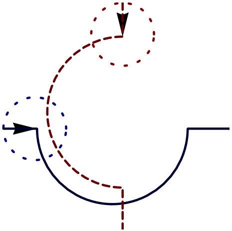




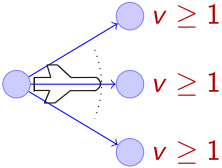
Logic for Hybrid Programs

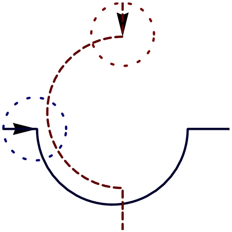
differential dynamic logic

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



$\vDash [d_1' = -\omega d_2, d_2' = \omega d_1]\, v \geq 1$

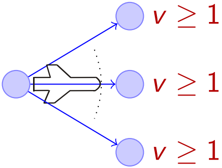




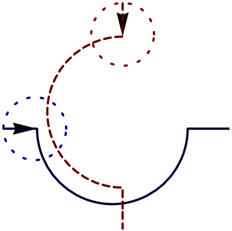
differential dynamic logic

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

$\vDash [\texttt{if}(x_1 > 0)\, \omega := 1;\ d_1' = -\omega d_2, d_2' = \omega d_1]\, v \geq 1$



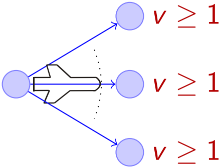
Logic for Hybrid Programs



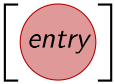
differential dynamic logic

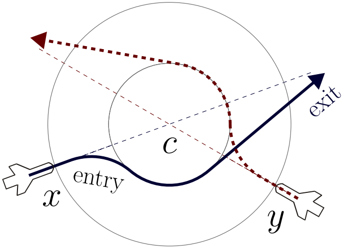
$$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$$

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



Logic for Compositional Verification



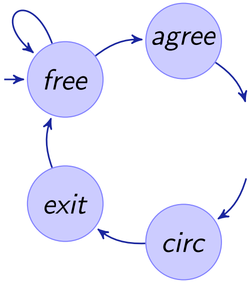


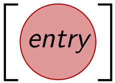
Example

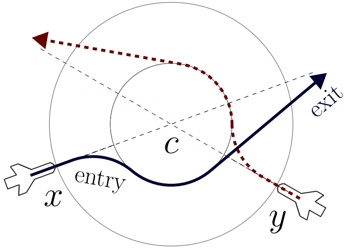
$$\mathit{safe} \land \mathit{far} \quad \rightarrow \quad [\mathit{entry}](\mathit{safe} \land \mathit{tangential})$$

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

Logic for Compositional Verification



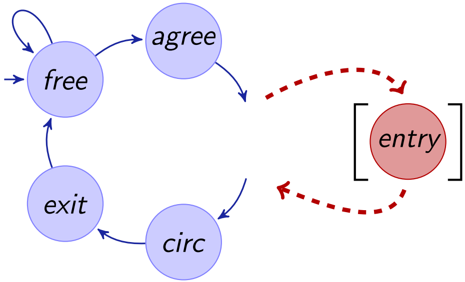


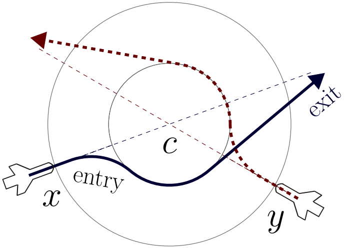


Example

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

Logic for Compositional Verification





Example

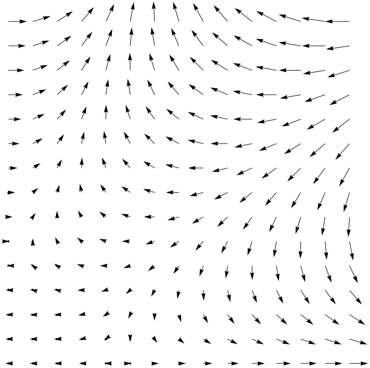
$$\begin{aligned} \mathit{safe} \land \mathit{far} &\rightarrow [\mathit{entry}](\mathit{safe} \land \mathit{tangential}) \\ \mathit{safe} \land \mathit{tangential} &\rightarrow [\mathit{other\ subsystem}]\mathit{safe} \\ \text{where}\ \ \mathit{safe} &\equiv (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2 \end{aligned}$$

} conjunction

Differential Invariants for Differential Equations

"Definition" (Differential Invariant)

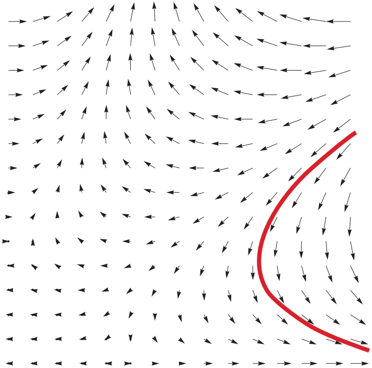
"Formula that remains true in the direction of the dynamics"



Differential Invariants for Differential Equations

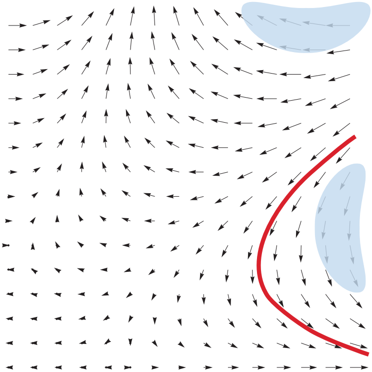
"Definition" (Differential Invariant)

"Formula that remains true in the direction of the dynamics"



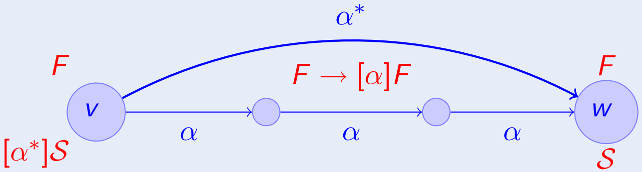
"Definition" (Differential Invariant)

"Formula that remains true in the direction of the dynamics"



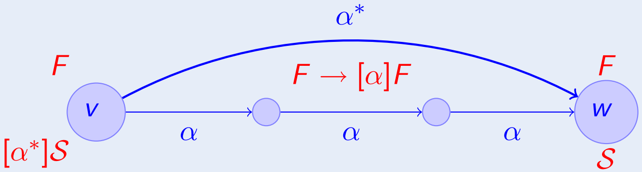
Discrete versus Differential Invariants

Definition (Discrete Invariant F)

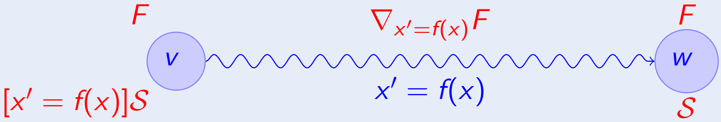


Discrete versus Differential Invariants

Definition (Discrete Invariant F)

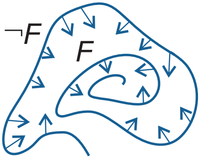


Definition (Differential Invariant F)

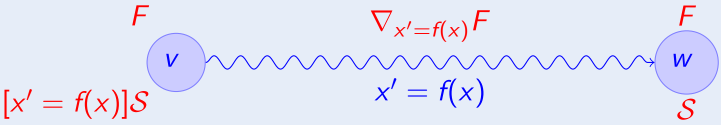


Discrete versus Differential Invariants

$$\nabla_{x_1'=f_1(x),\dots,x_n'=f_n(x)} F \quad \text{is} \quad \bigwedge_{(b\geq c)\in F} \left(\sum_{i=1}^{n} \frac{\partial b}{\partial x_i} f_i(x) \geq \sum_{i=1}^{n} \frac{\partial c}{\partial x_i} f_i(x) \right)$$

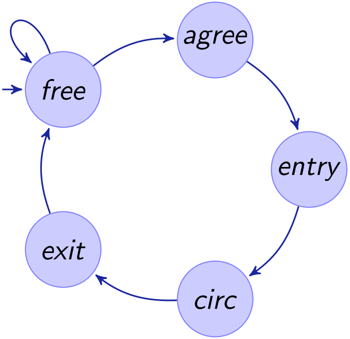


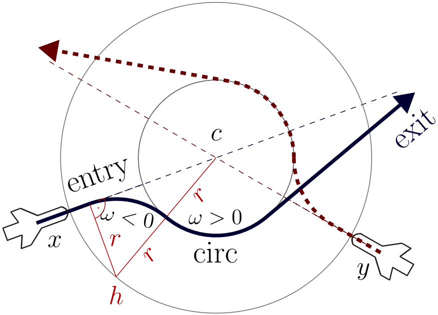
Definition (Differential Invariant F)



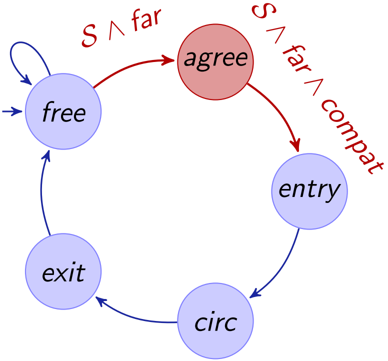
Outline

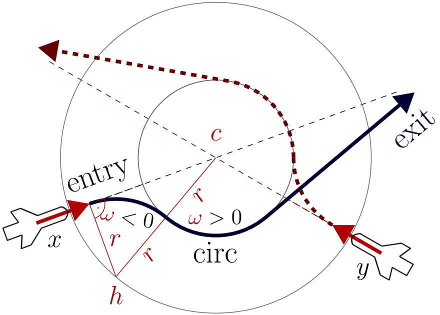
Verification Loop for Air Traffic Control





Verification Loop for Air Traffic Control

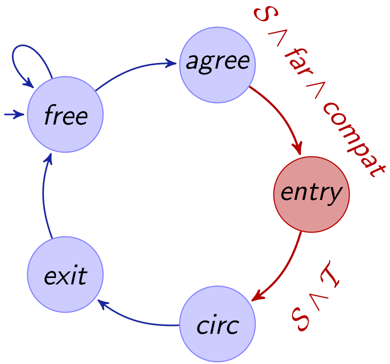


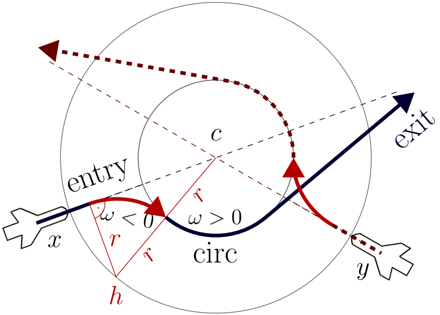


Example (dℒ formula of verification subgoal)

$$\textit{safe} \land \textit{far} \;\rightarrow\; [\textit{agree}](\textit{safe} \land \textit{far} \land \textit{compatible})$$

Verification Loop for Air Traffic Control

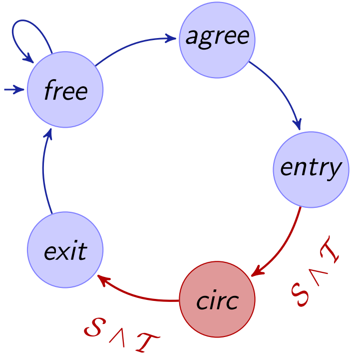


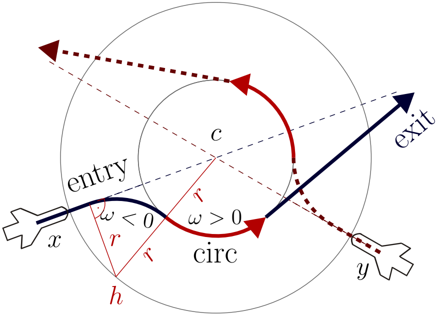


Example (d$\mathcal{L}$ formula of verification subgoal)

$$\textit{safe} \land \textit{far} \land \textit{compatible} \rightarrow [\textit{entry}](\textit{safe} \land \textit{tangential})$$

Verification Loop for Air Traffic Control

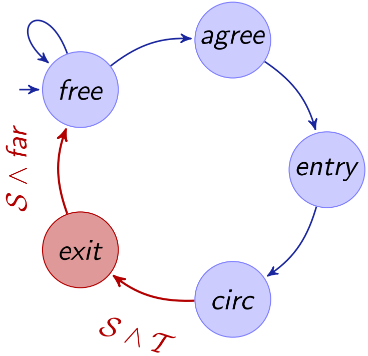


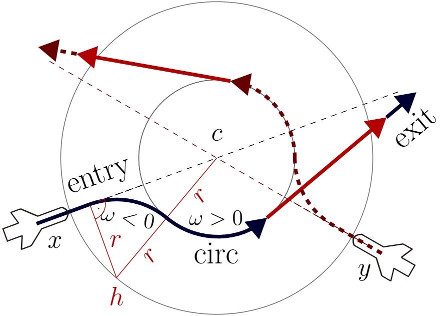


Example (d$\mathcal{L}$ formula of verification subgoal)

$$\mathit{safe} \wedge \mathit{tangential} \rightarrow [\mathit{circ}](\mathit{safe} \wedge \mathit{tangential})$$

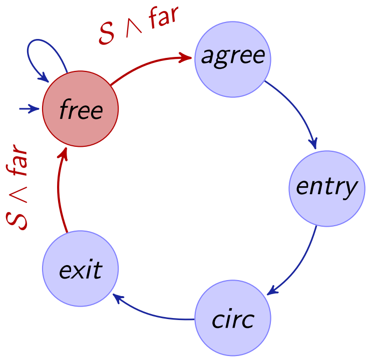
Verification Loop for Air Traffic Control

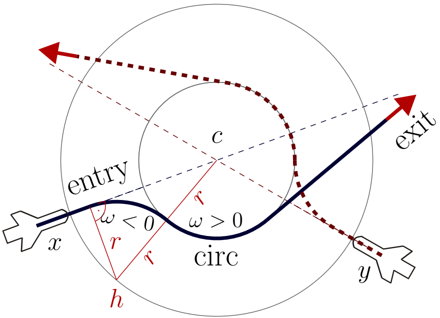




Example (d$\mathcal{L}$ formula of verification subgoal)

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

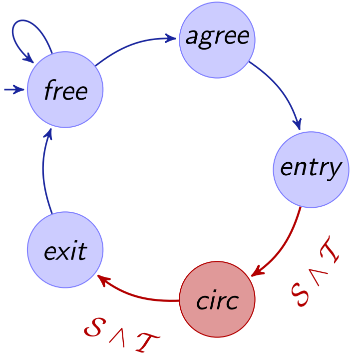


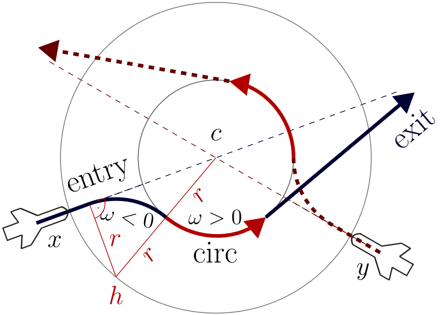


Example (d$\mathcal{L}$ formula of verification subgoal)

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

Verification Loop for Air Traffic Control



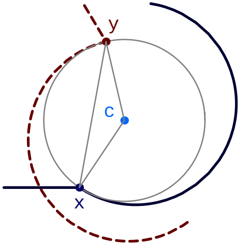


Example (d$\mathcal{L}$ formula of verification subgoal)

$$\mathit{safe} \wedge \mathit{tangential} \;\rightarrow\; [\mathit{circ}](\mathit{safe} \wedge \mathit{tangential})$$

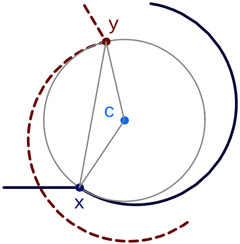
Verify Roundabout Flight with Differential Invariants

$$\overline{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1 \ldots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



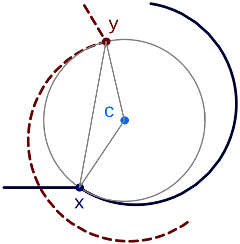
Verify Roundabout Flight with Differential Invariants

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

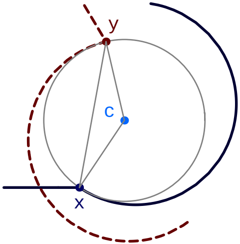


Verify Roundabout Flight with Differential Invariants

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



$$\frac{\dfrac{\partial\|x-y\|^2}{\partial x_1}d_1 + \dfrac{\partial\|x-y\|^2}{\partial y_1}e_1 + \dfrac{\partial\|x-y\|^2}{\partial x_2}d_2 + \dfrac{\partial\|x-y\|^2}{\partial y_2}e_2 \geq \dfrac{\partial p^2}{\partial x_1}d_1 \ldots}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1 \ldots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$

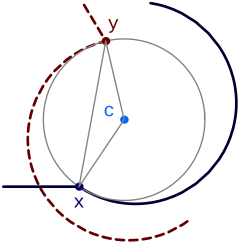


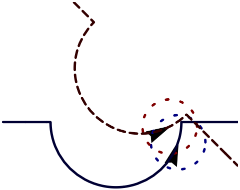
Verify Roundabout Flight with Differential Invariants

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

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

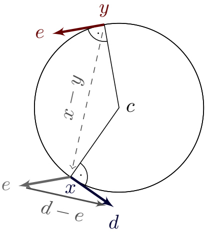
$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1 \dots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

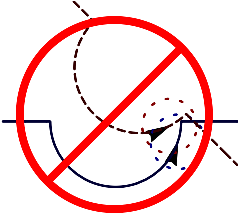




Verify Roundabout Flight with Differential Invariants

$$\dfrac{\dfrac{2(x_1 - y_1)\color{red}{(d_1 - e_1)} + 2(x_2 - y_2)\color{red}{(d_2 - e_2)} \geq 0}{\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1 \ldots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$





$$\overline{[d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1 ..]\color{red}{d_1 - e_1 = -\omega(x_2 - y_2)}}$$

Verify Roundabout Flight with Differential Invariants

$$\cfrac{\cfrac{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1\dots](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$

Proposition (Differential saturation)

F differential invariant of $x'=\theta\wedge H$, then
$x'=\theta\wedge H$ equivalent to $x'=\theta\wedge H\wedge F$

$$\cfrac{}{[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1..]d_1-e_1=-\omega(x_2-y_2)}$$

Verify Roundabout Flight with Differential Invariants

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

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

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

$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1 \ldots](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

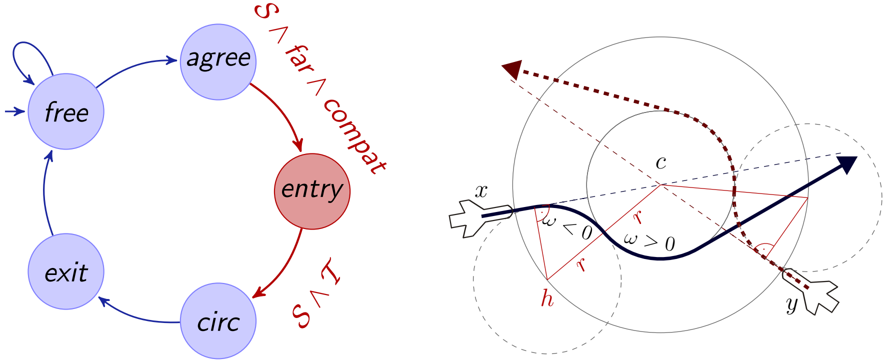
Proposition (Differential saturation)

F differential invariant of $x' = \theta \land H$, then

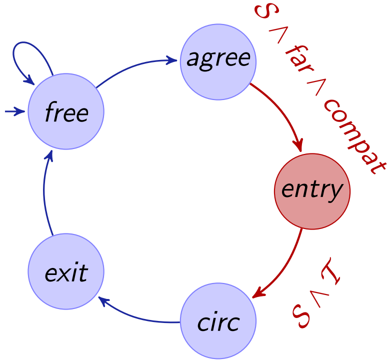
$$x' = \theta \land H \quad \text{equivalent to} \quad x' = \theta \land H \land F$$

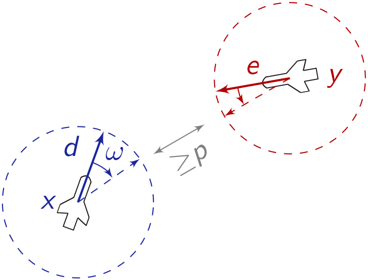
$$[d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1 ..] d_1 - e_1 = -\omega(x_2 - y_2)$$

Flyable Roundabout Maneuver: Entry

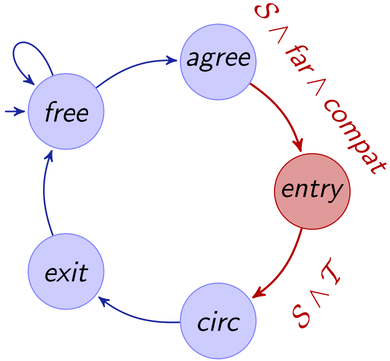


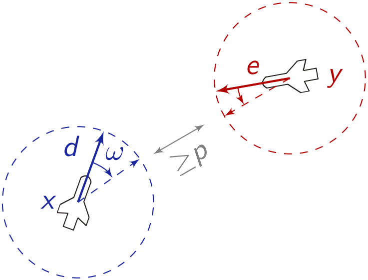
Flyable Roundabout Maneuver: Entry



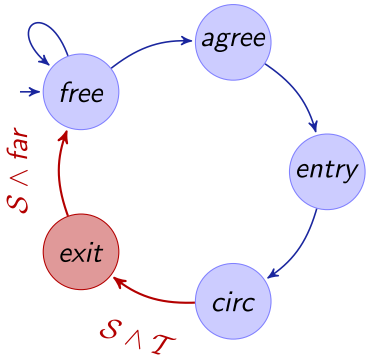


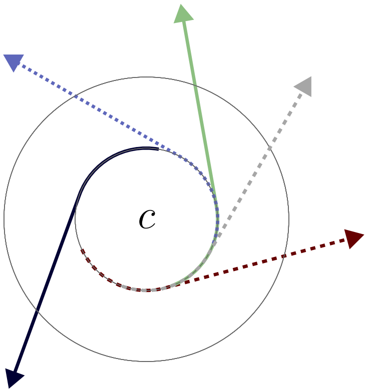
Flyable Roundabout Maneuver: Entry



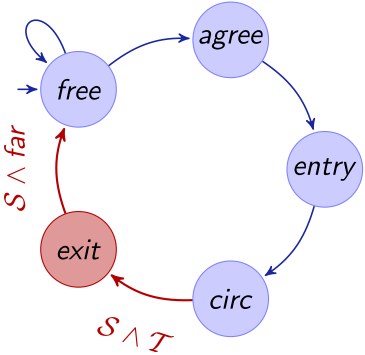


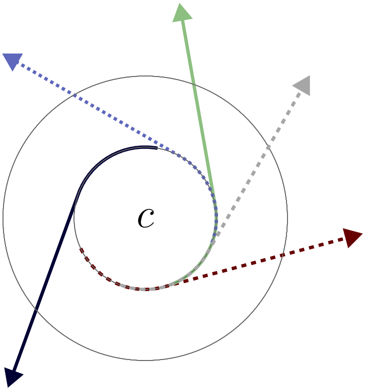
Flyable Roundabout Maneuver: Exit



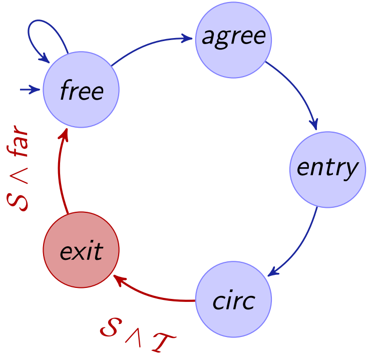


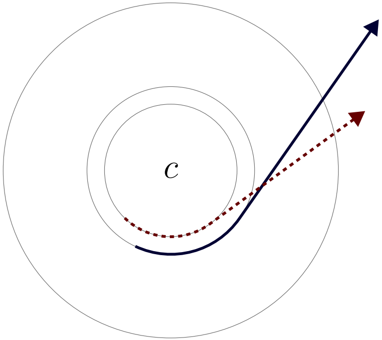
Flyable Roundabout Maneuver: Exit



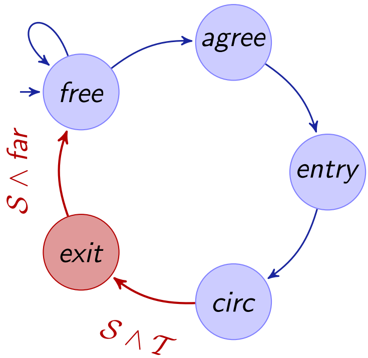


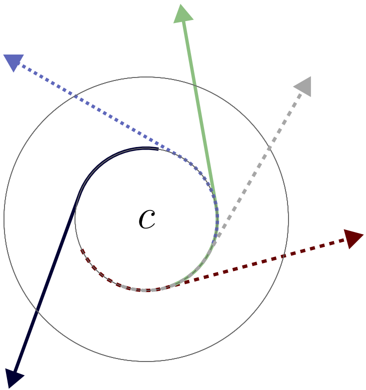
Flyable Roundabout Maneuver: Exit





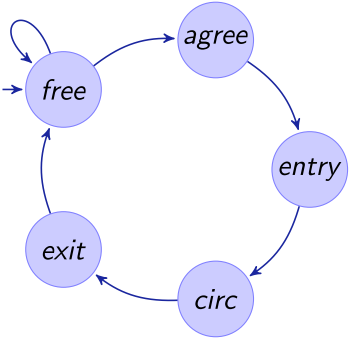
Flyable Roundabout Maneuver: Exit

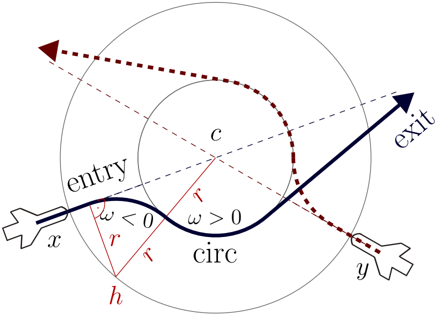




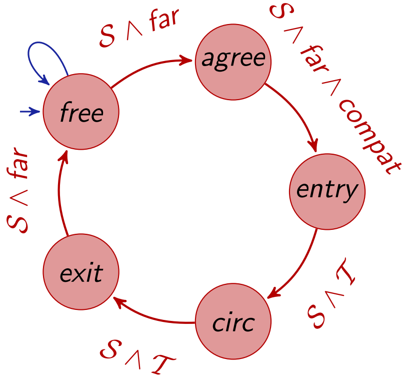
Outline

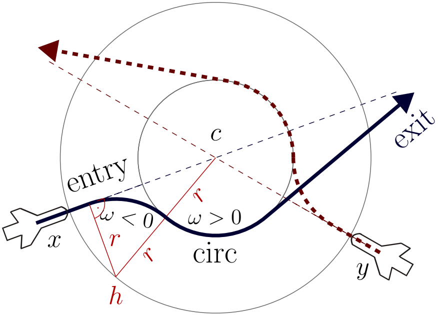
Flyable Roundabout Maneuver: Summary



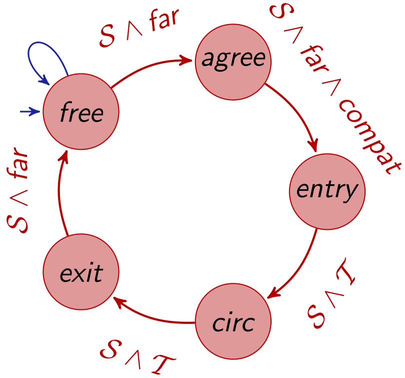


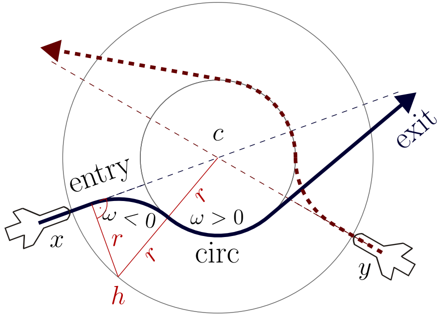
Flyable Roundabout Maneuver: Summary





Flyable Roundabout Maneuver: Summary





Theorem (Collision freedom)

FTRM is collision free:

$$\|x - y\| \geq far \land \ldots \to [FTRM]\|x - y\| \geq p$$

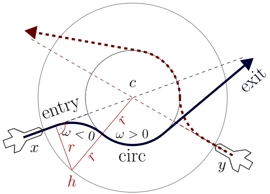
Outline

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

Outline

Conclusions & Future Work



- Formal verification can scale to real aircraft maneuvers!
- Differential invariants instead of reachability along solutions
- Fixedpoint computations to find differential invariants
- Compositional verification
- Challenging arithmetic complexity (simplifications)

- Improve differential invariant generation
- Abstract interpretation domain
- Widening in fixedpoint loop
- Nonlinear real arithmetic