Formalizing Hybrid Systems with Event-B

Jean-Raymond Abrial, Wen Su, Huibiao Zhu

August 2012

Prologue

Using B Formal Method in Industry

- Fully automatic train systems:
    - Paris metro line 14 (October 1998)
    - Roissy airport shuttle (March 2007)
- More train applications

Paris Metro Line 14 (Source: Siemens)

Line length	8.5 km
Number of Stops	8
Time interval between two trains	115 s
Speed	40 km/h
Number of trains	17
Passengers per day	350,000

Roissy Airport Shuttle (Source: Siemens)

Line length	3.3 km
Number of Stops	5
Time interval between two trains	105 s
Speed	26 km/h
Number of trains	14
Passengers per hour	$2,000$

Comparing the Case Studies (1)

	Paris	Roissy
Number of final ADA lines (from B)	$86,000$	$158,000$
Number of proofs	$27,800$	$43,610$
Percentage of interactive proofs	8.1	3.3
Interactive proofs in Man.Month	7.1	4.6

Comparing the Case Studies (2)

- Man.month calculated with:
    - 15 interactive proofs per man.day
    - 21 days in a month

- In both cases, no unit tests and no integration tests

- Reinforcing global tests (catastrophic scenarios)

-Important differences in the software requirements:
    - Paris: specially done for the project
    - Paris: adaptation from O'Hare Airport (problems)

Similar Applications by Siemens (1)

City	Line	Service	Driverless
Algiers	1	2011	No
Barcelona	9	2007	Yes
Budapest	4	2013	Yes
Caracas	4	2004	No
Helsinki	1	2013	No
Hong Kong	TKO	2001	No

Similar Applications by Siemens (2)

City	Line	Service	Driverless
Mexico	B	2000	No
New York	Canarsie	2006	No
	PATH	2014	No
Paris	14	1998	Yes
	3	2009	No
	1	2011	Yes
	5	2012	No

Similar Applications by Siemens (3)

City	Line	Service	Driverless
Rennes	B	2018	Yes
Roissy CDG	1	2007	Yes
	2	2007	Yes
San Juan	2	2004	No
Sao Paulo	TKO	2001	Yes

Contact: <Jean-Marc.Meynadier@siemens.com>

Similar Applications by Alstom (1)

System	City	Service	Size	Language	Driverless
KVB	French Trains	1993	30000	ADA	No
CDTC	Cairo	1996	3000	Modula2	No
SACEM	Paris (RER B)	1996	2500	Modula2	No
ACSES	AMTRACK (USA)	2002	14500	ADA	No

Similar Applications by Alstom (2)

System	City	Service	Size	Language	Driverless
Urbalis 200	Shanghai	2003	30000	ADA	No
	New Dehli				
	Seoul				
	Daegu				
	Incheoun				
	Madrid				
	Santiago				
	Cairo	2013			
	Bangalore				
	Calcutta				

Similar Applications by Alstom (3)

System	City	Service	Size	Language	Driverless
Urbalis 400	Shanghai	2008	100000	ADA	No
	Beijing				Yes
	Chenzen				No
	Sao Paulo	2013			Yes
	Mexico				No
	Milano				No
	Toronto				No
	Wuhan				No

Contact: <Luis-Fernando.Mejia@transport.alstom.com>

Formalizing Hybrid Systems with Event-B

Jean-Raymond Abrial, Wen Su, Huibiao Zhu

August 2012

- Event-B is said to handle discrete transition systems: is it enough?

- Event-B is said to handle discrete transition systems: is it enough?

- Continuous transition systems are important too

- Event-B is said to handle discrete transition systems: is it enough?

- Continuous transition systems are important too: are not they?

- Event-B is said to handle discrete transition systems: is it enough?

- Continuous transition systems are important too: are not they?

- How can time be handled in Event-B?

Frequently Asked Questions about Event-B

- Event-B is said to handle discrete transition systems: is it enough?

- Continuous transition systems are important too: are not they?

- How can time be handled in Event-B?

- Is it necessary to add a special "time feature" within Event-B?

Frequently Asked Questions about Event-B

- Event-B is said to handle discrete transition systems: is it enough?

- Continuous transition systems are important too: are not they?

- How can time be handled in Event-B?

- Is it necessary to add a special "time feature" within Event-B?

- The idea is then to introduce (somehow) continuous transitions

- The idea is then to introduce (somehow) continuous transitions

- BUT, when introducing such continuous transitions

- The idea is then to introduce (somehow) continuous transitions

- BUT, when introducing such continuous transitions

  the discrete transitions are still needed

- The idea is then to introduce (somehow) continuous transitions

- BUT, when introducing such continuous transitions

  the discrete transitions are still needed

- Hence the notion of hybrid systems

- The idea is then to introduce (somehow) continuous transitions

- BUT, when introducing such continuous transitions

  the discrete transitions are still needed

- Hence the notion of hybrid systems

  where both discrete and continuous transitions can occur

Typical Hybrid Systems

- Hybrid frameworks are frequent in embedded systems where:

Typical Hybrid Systems

- Hybrid frameworks are frequent in embedded systems where:
    - A piece of software, the controller, manages an environment

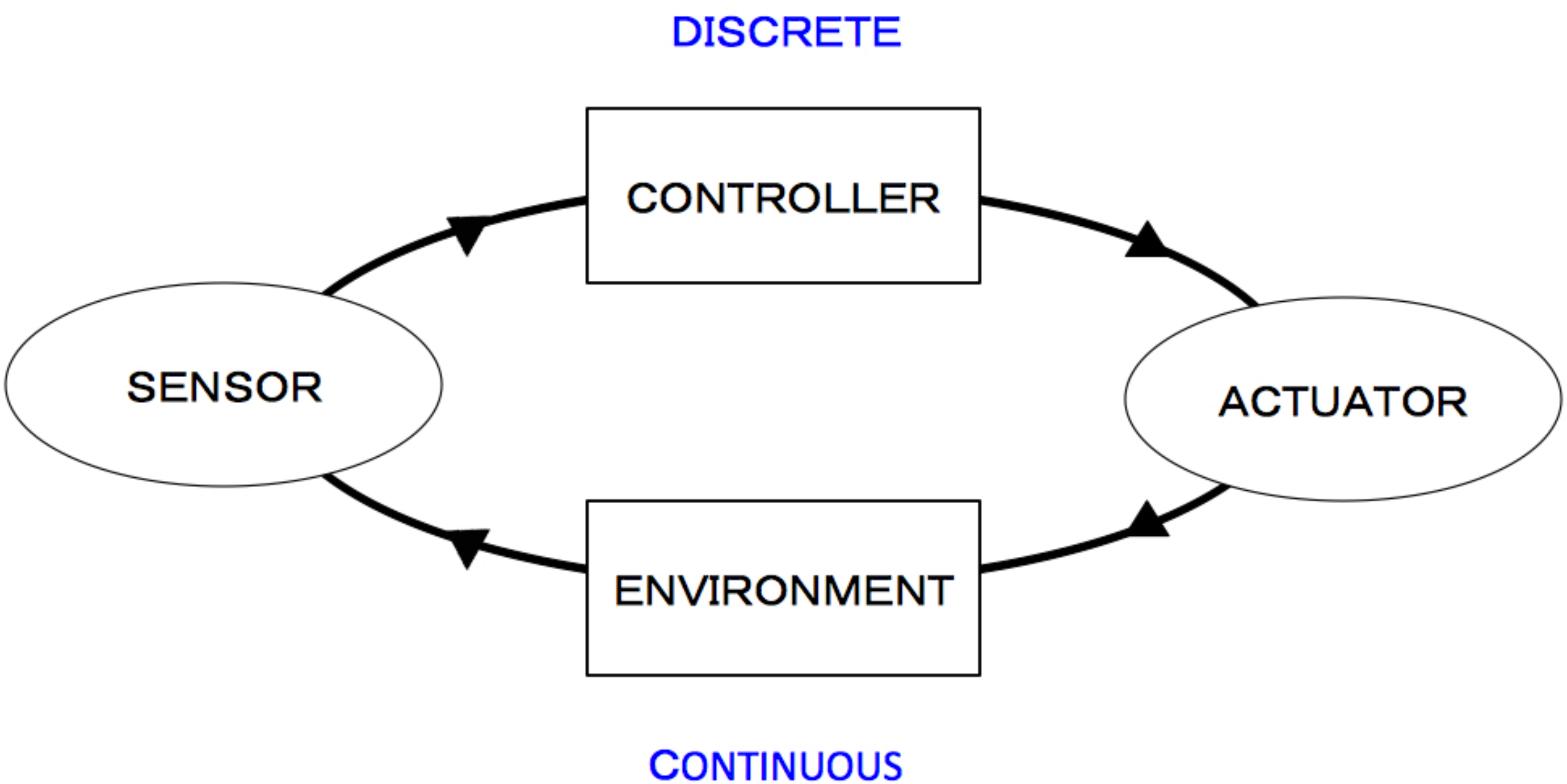
- Hybrid frameworks are frequent in embedded systems where:
    - A piece of software, the controller, manages an environment
    - Controller is linked to environment by sensors and actuators

- Hybrid frameworks are frequent in embedded systems where:
    - A piece of software, the controller, manages an environment
    - Controller is linked to environment by sensors and actuators
    - Controller works from time to time in a DISCRETE fashion

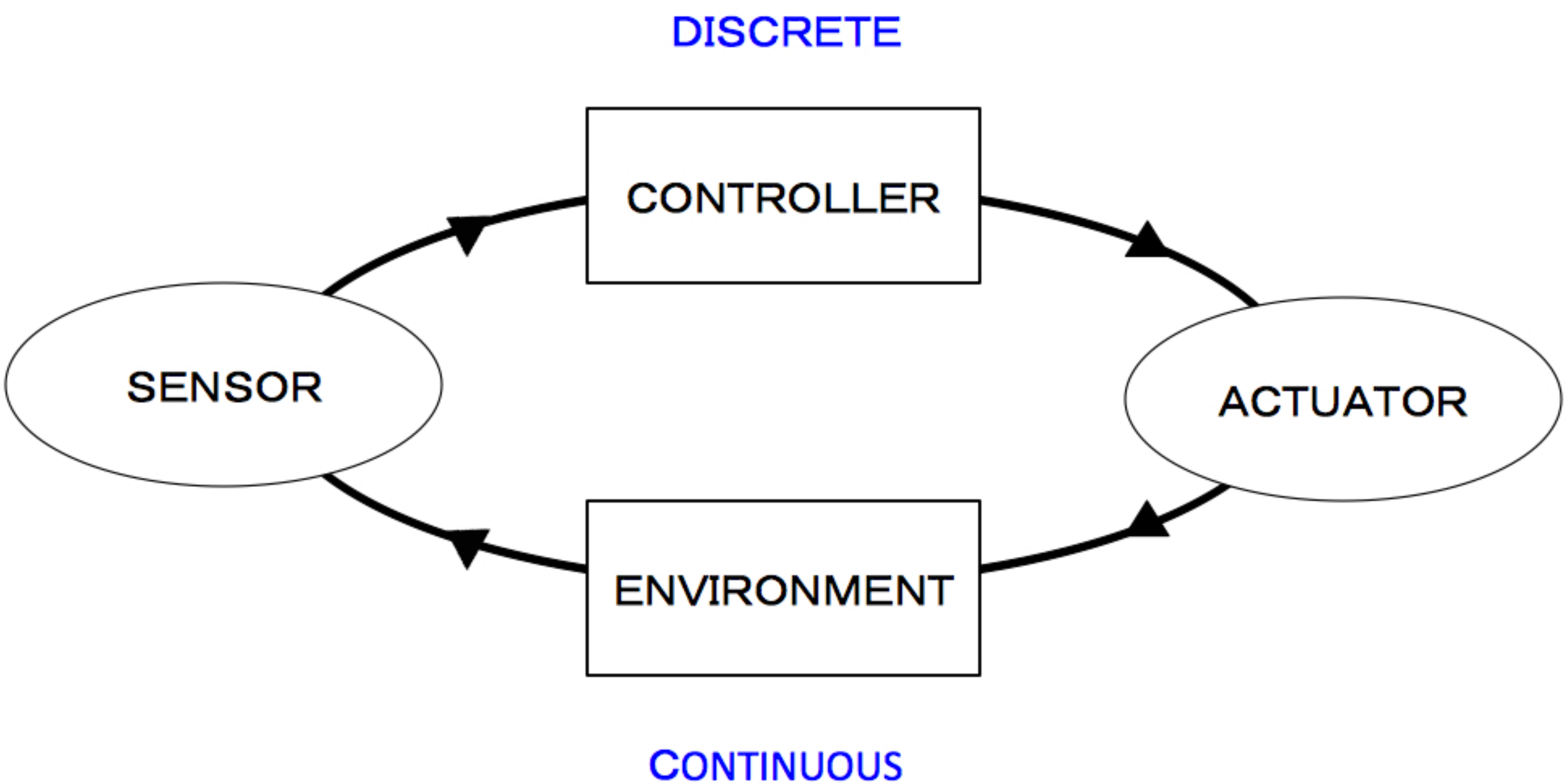
Typical Hybrid Systems

- Hybrid frameworks are frequent in embedded systems where:
  - A piece of software, the controller, manages an environment
  - Controller is linked to environment by sensors and actuators
  - Controller works from time to time in a DISCRETE fashion
  - While environment evolves in a CONTINUOUS way.

Illustration

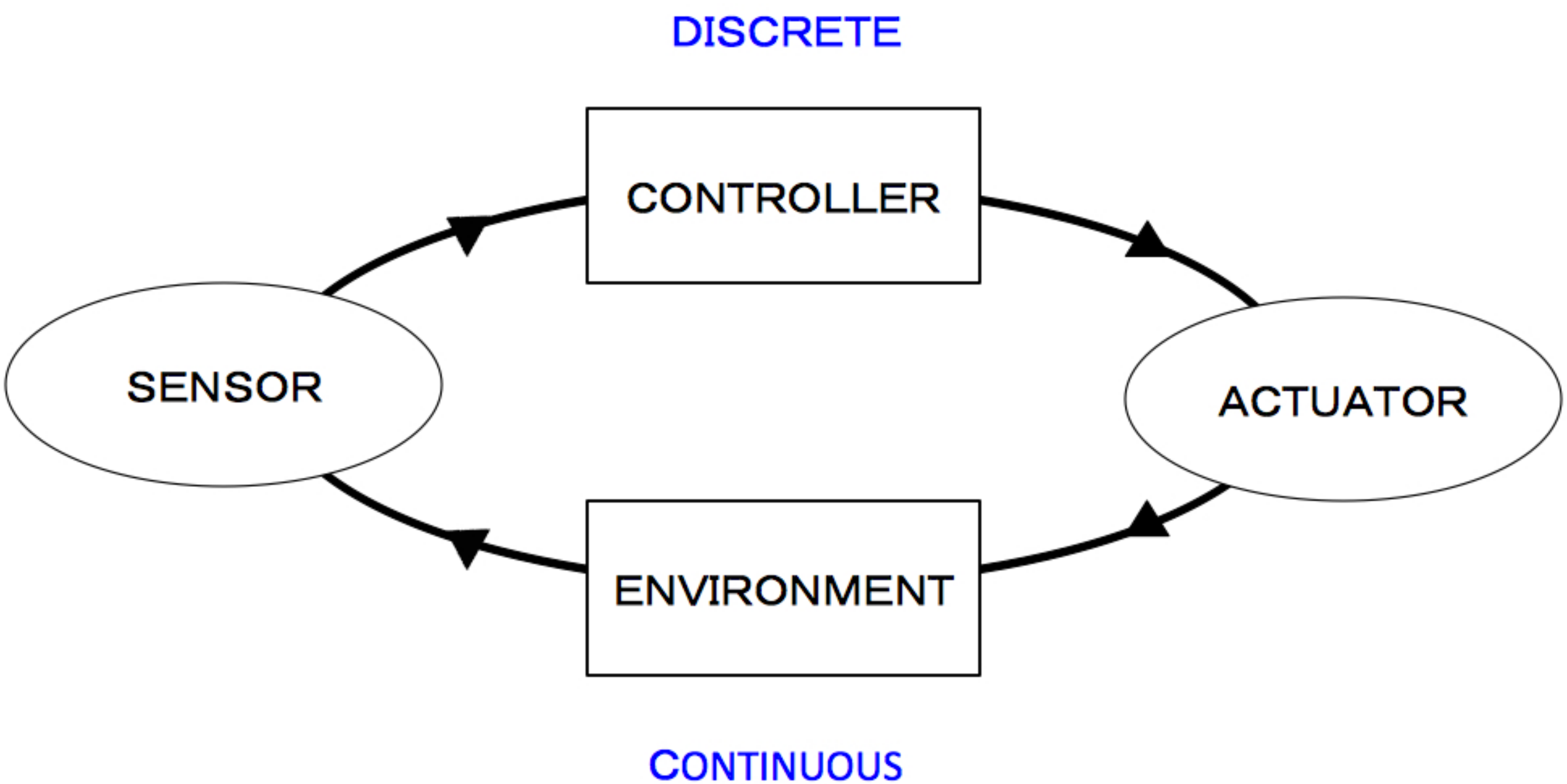


Illustration



- We want to develop models of such closed systems

Illustration



- We want to develop models of such closed systems

- We have thus to cope with both discrete and continuous evolutions

Example

- Continuous physical environment:

  a train defined by its position, speed, and acceleration

- Continuous physical environment:

a train defined by its position, speed, and acceleration

- Discrete controller:

  a driver changing from time to time the acceleration of the train

- Discrete controller:

  a driver changing from time to time the acceleration of the train

- Discrete controller:

  a driver changing from time to time the acceleration of the train

- Goal: to control the speed of the train (station or another train)

Our Approach was influenced by that of Action System

R.J. Back and R. Kurki-Suonio.

Distributed Cooperation with Action Systems

ACM Transaction on Programming Languages and Systems. 1988.

R.J. Back, L. Petre, and I. Porres.

Generalizing Action Systems to Hybrid Systems.

FTRTFT 2000. LNCS 1926 Springer Verlag, 2000.

R.J. Back, C. Cerschi Seceleanu, and J. Westerholm.

Symbolic Simulation of Hybrid Systems.

APSEC'02, 2002.

Our Papers

Formalizing Hybrid Systems with Event-B

ABZ Conference. Pisa, June 2012

Complementary Methodologies for Developing Hybrid Systems with Event-B

Accepted at ICFEM 2012. Kyoto, November 2012

The Approach with Event-B (inspired by Action System)

The Approach with Event-B (inspired by Action System)

- Discrete variables together with continuous variables

The Approach with Event-B (inspired by Action System)

- Discrete variables together with continuous variables

- Continuous variables are time functions as in Action System

The Approach with Event-B (inspired by Action System)

- Discrete variables together with continuous variables

- Continuous variables are time functions as in Action System

- We are interested in the immediate future of continuous variables

The Approach with Event-B (inspired by Action System)

- Discrete variables together with continuous variables

- Continuous variables are time functions as in Action System

- We are interested in the immediate future of continuous variables

- Discrete systems as an abstraction of continuous ones

The Approach with Event-B (inspired by Action System)

- Discrete variables together with continuous variables

- Continuous variables are time functions as in Action System

- We are interested in the immediate future of continuous variables

- Discrete systems as an abstraction of continuous ones

- We thus use refinement from a discrete to a continuous system

Three Examples

- The 2 examples:
  - Aircraft collision avoidance
  - Train control (time permitting),

- The 2 examples:
  - Aircraft collision avoidance
  - Train control (time permitting),
- Description:
  - The problem,
  - The constraints and goal,
  - The solution,
  - The discrete and continuous transitions

Two Examples

- The 2 examples:
  - Aircraft collision avoidance
  - Train control (time permitting),
- Description:
  - The problem,
  - The constraints and goal,
  - The solution,
  - The discrete and continuous transitions
- Examples developed and fully proved with the Rodin Platform

- The 2 examples:
    - Aircraft collision avoidance
    - Train control (time permitting),
- Description:
    - The problem,
    - The constraints and goal,
    - The solution,
    - The discrete and continuous transitions
- Examples developed and fully proved with the Rodin Platform
- These examples show complete analytical solutions

Example 1

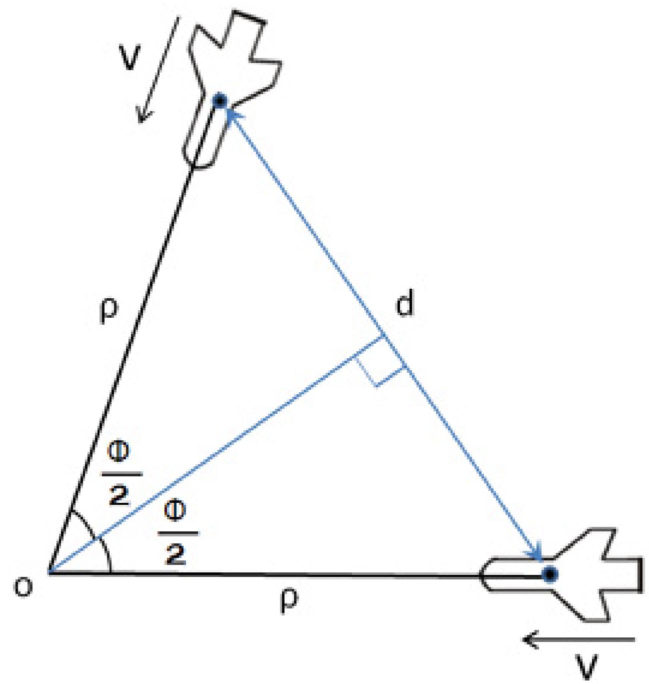
- Two aircrafts are flying at the same altitude and speed

- Two aircrafts are flying at the same altitude and speed

- They might converge (collision) at some point o

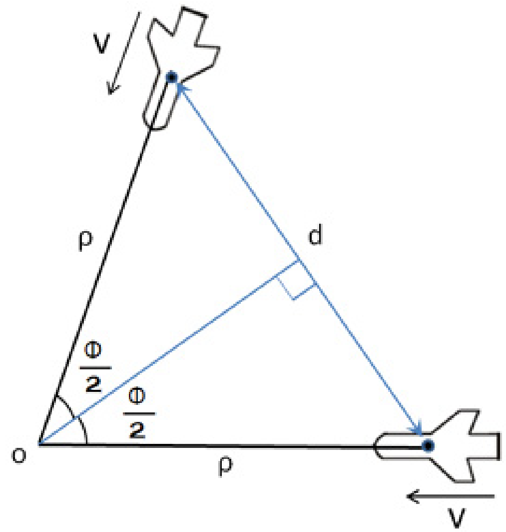
- Two aircrafts are flying at the same altitude and speed

- They might converge (collision) at some point o



Aircraft Collision Avoidance: Constraint and goal

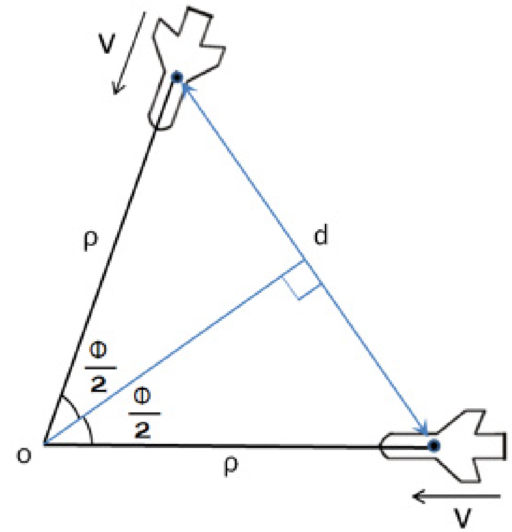
Aircraft Collision Avoidance: Constraint and goal



- The distance between aircrafts is as follows:

$$d = 2\rho \sin \frac{\phi}{2}$$

Aircraft Collision Avoidance: Constraint and goal

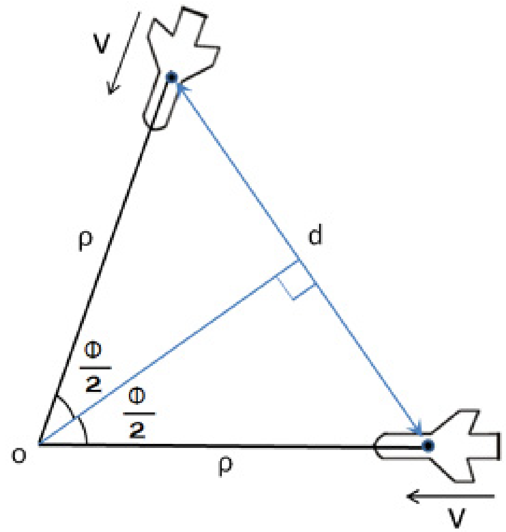


- The distance between aircrafts is as follows:

$$d = 2\rho \sin\frac{\phi}{2}$$

- Their distance must always be greater than or equal to a constant p

Aircraft Collision Avoidance: Constraint and goal



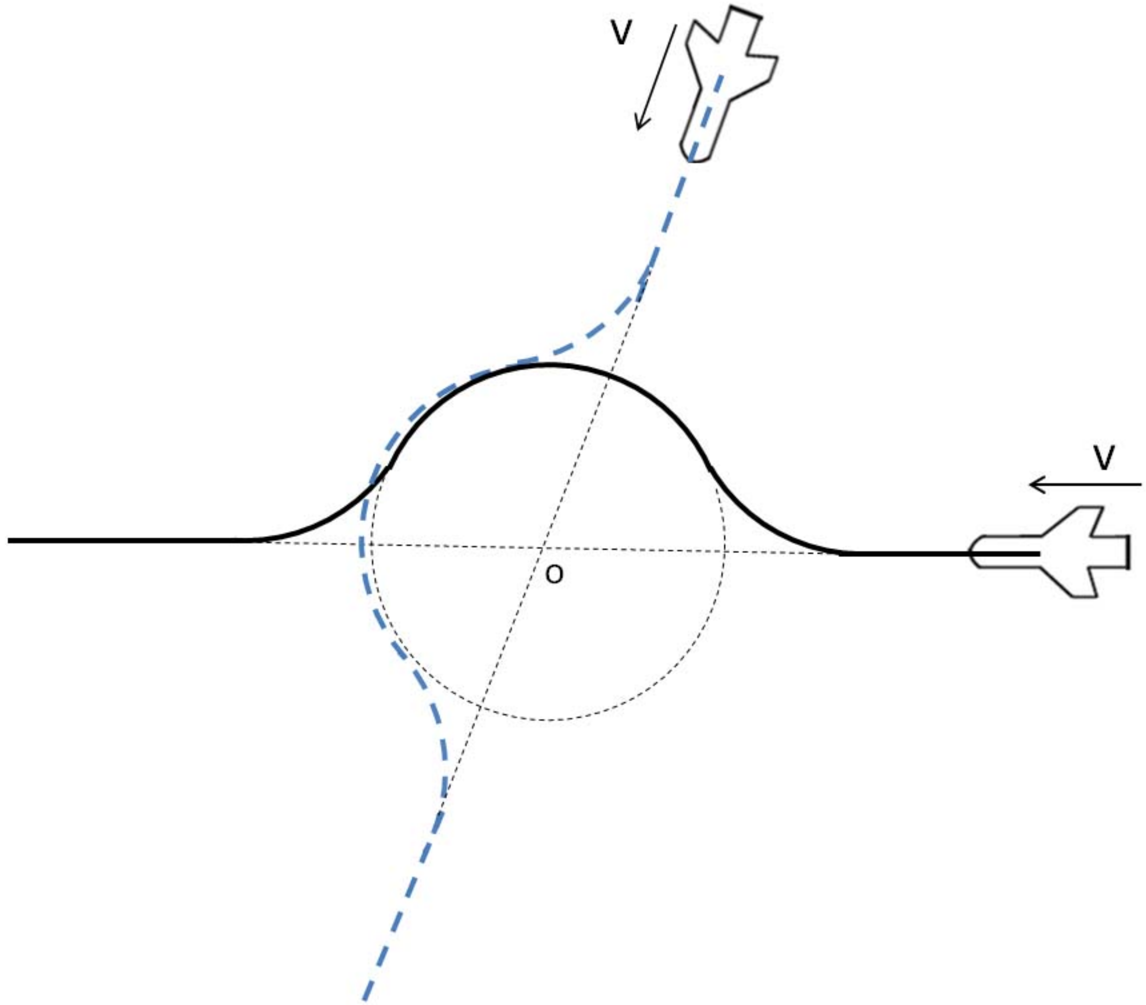
- The distance between aircrafts is as follows:

$$d = 2\rho \sin \frac{\phi}{2}$$

- Their distance must always be greater than or equal to a constant p

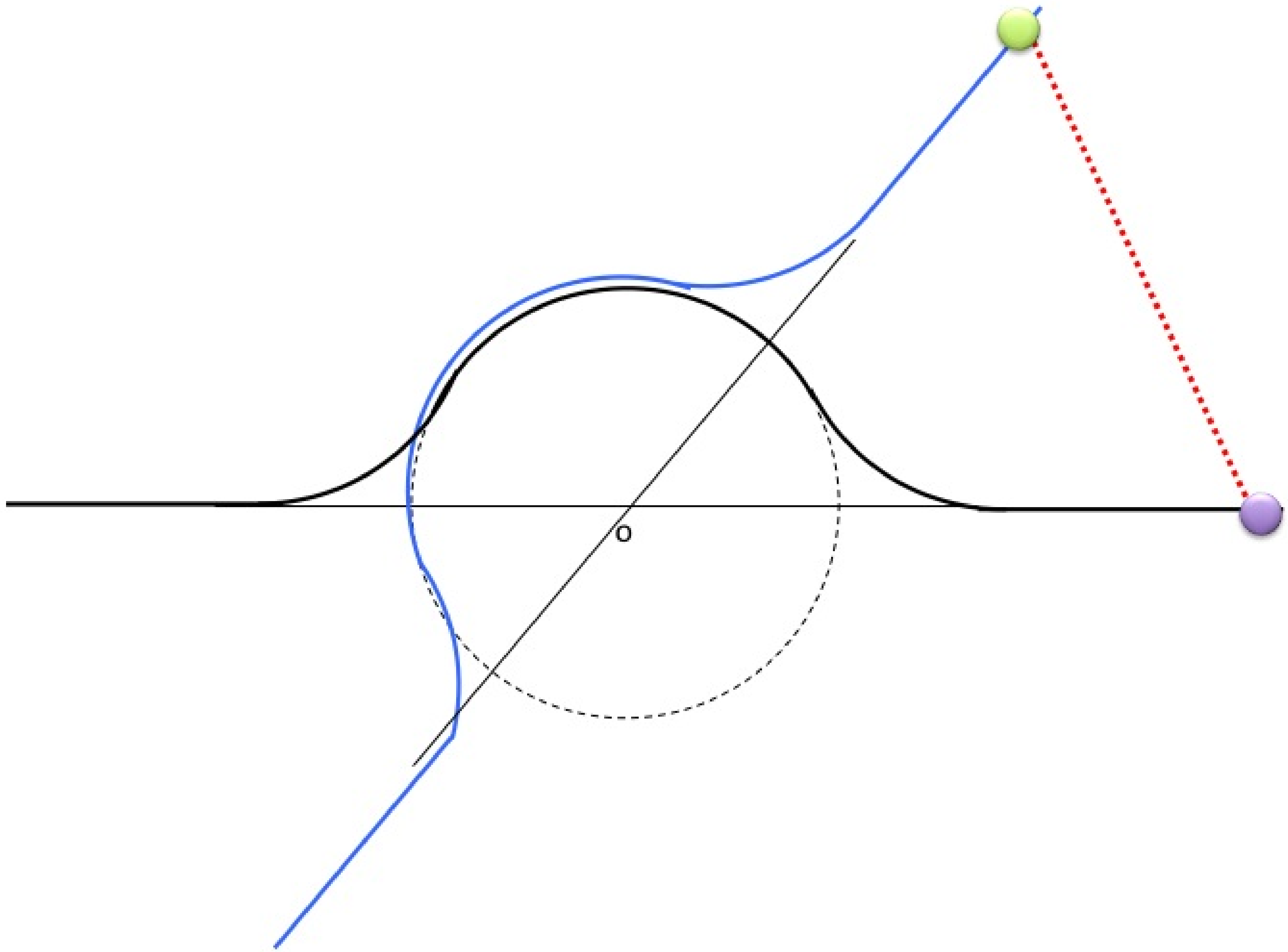
- Goal: we want to find a solution to avoid the collision

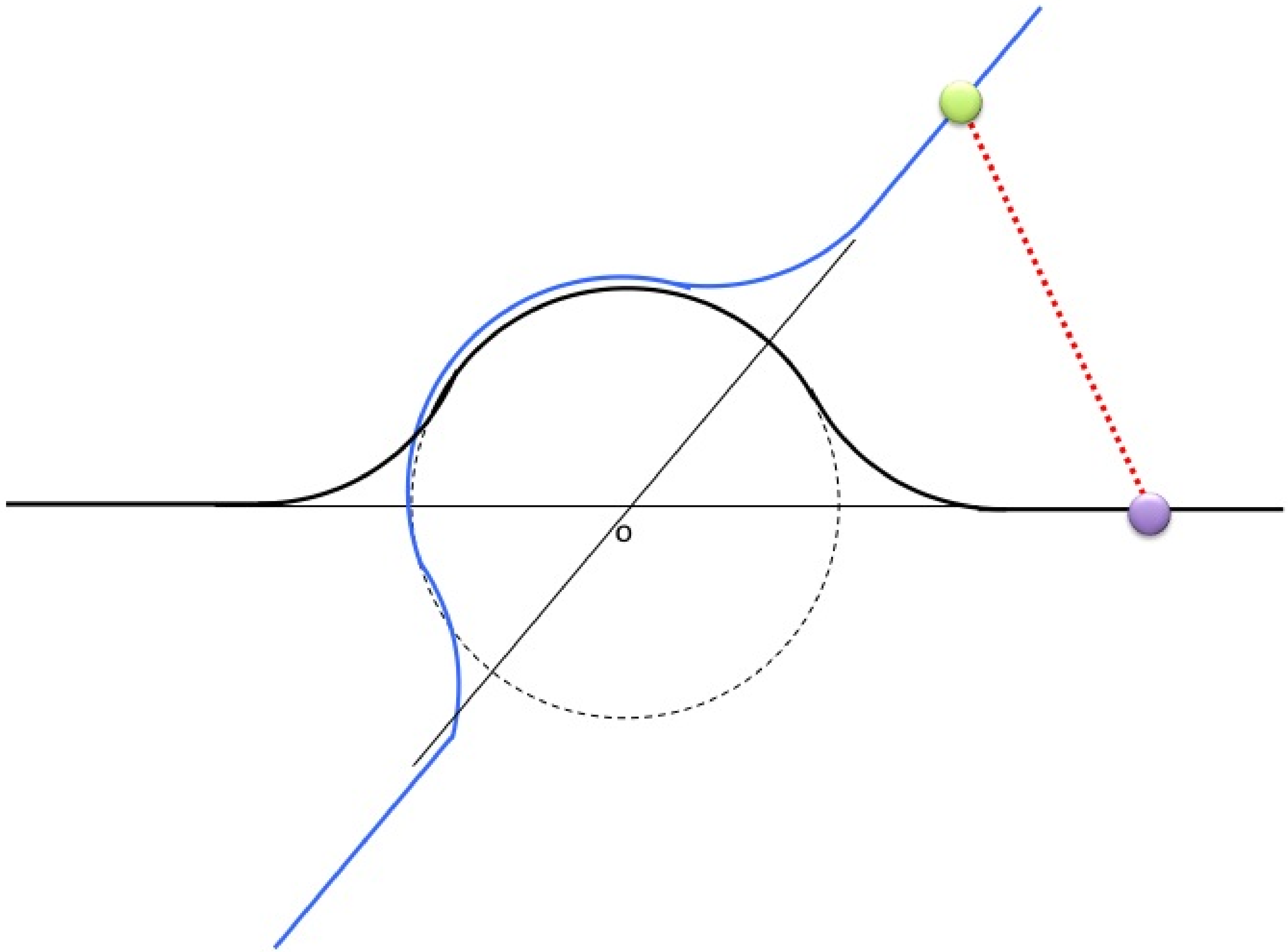
The Solution

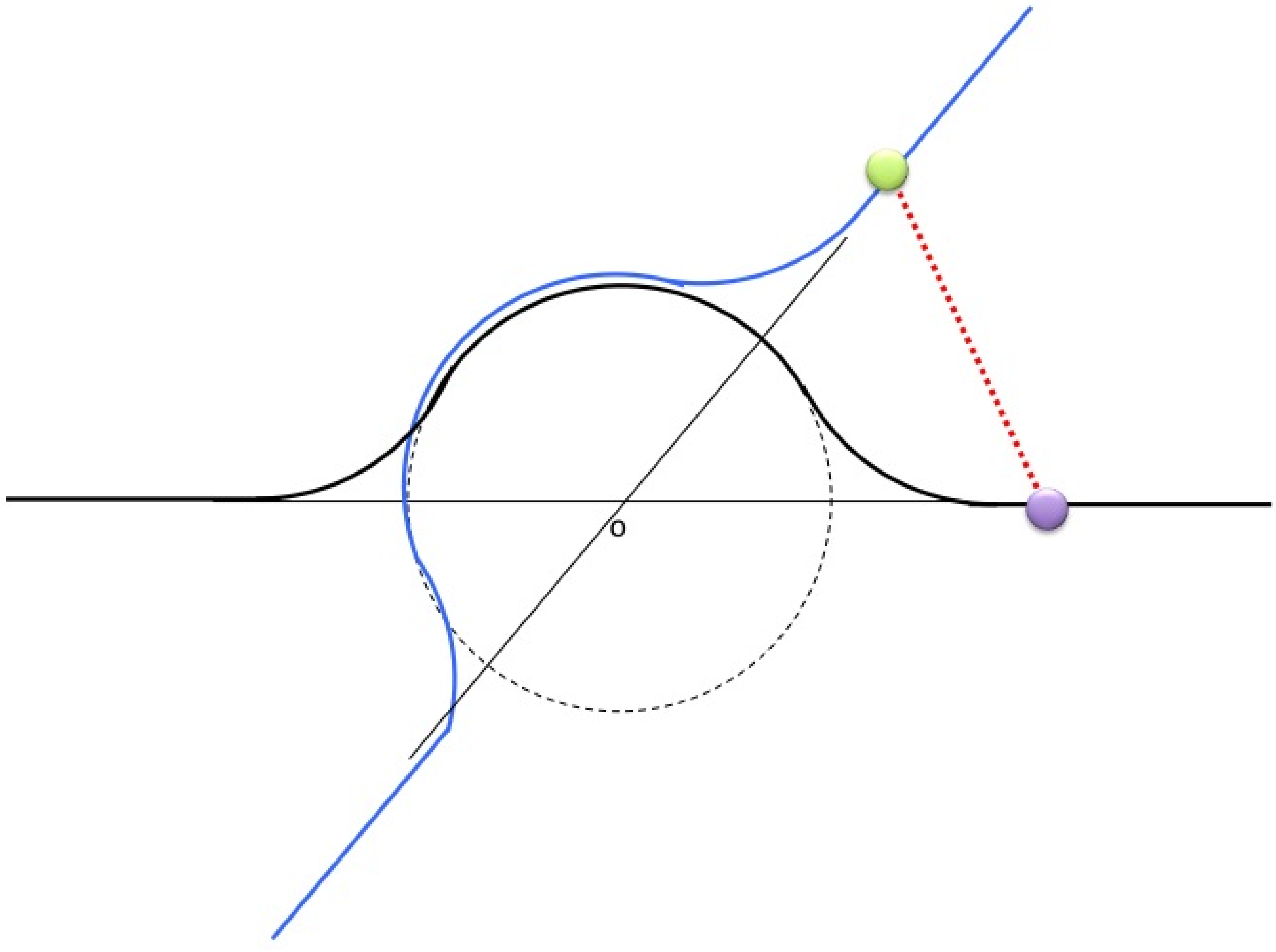


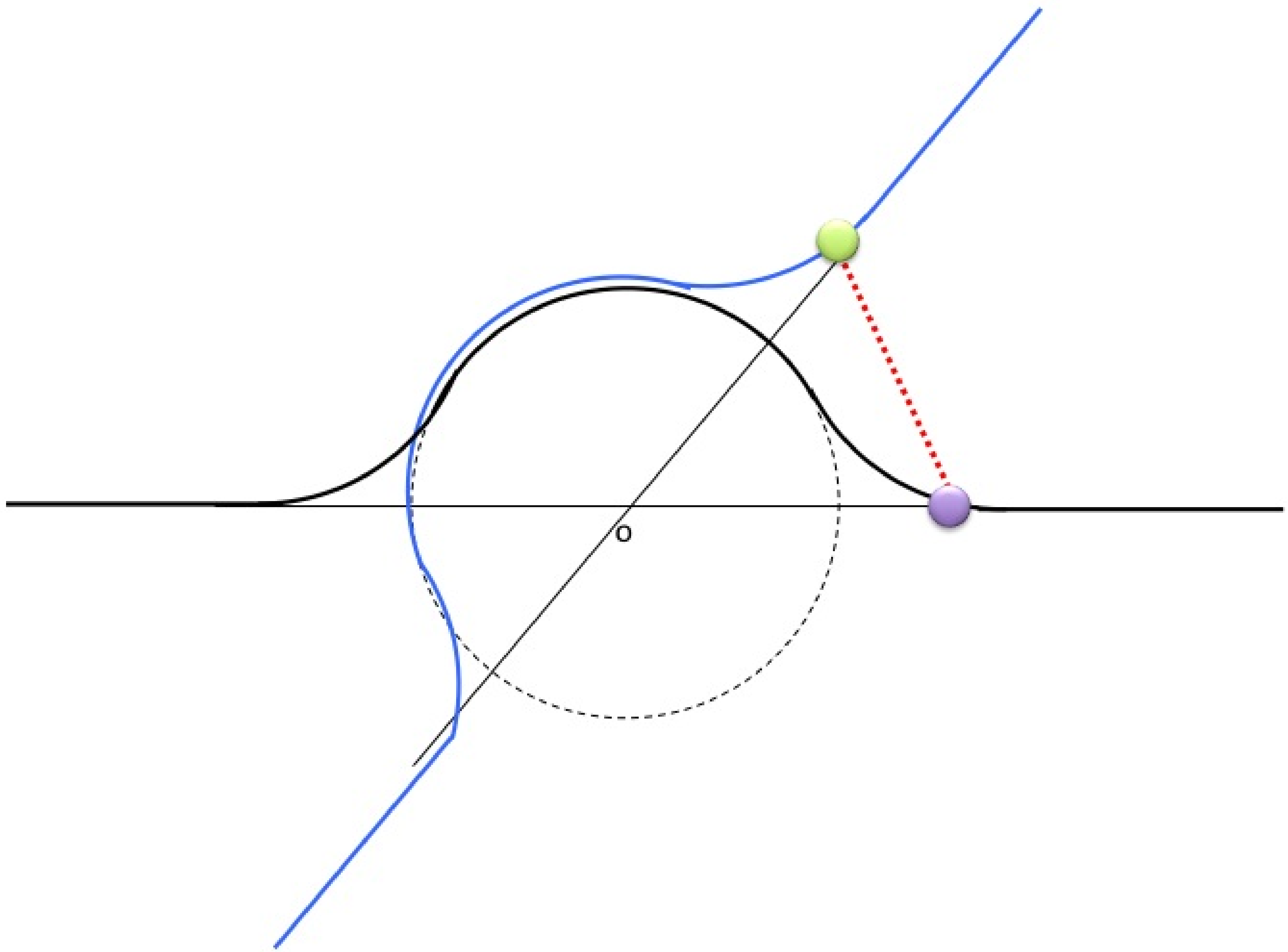
- The radius r of this circle will be determined later

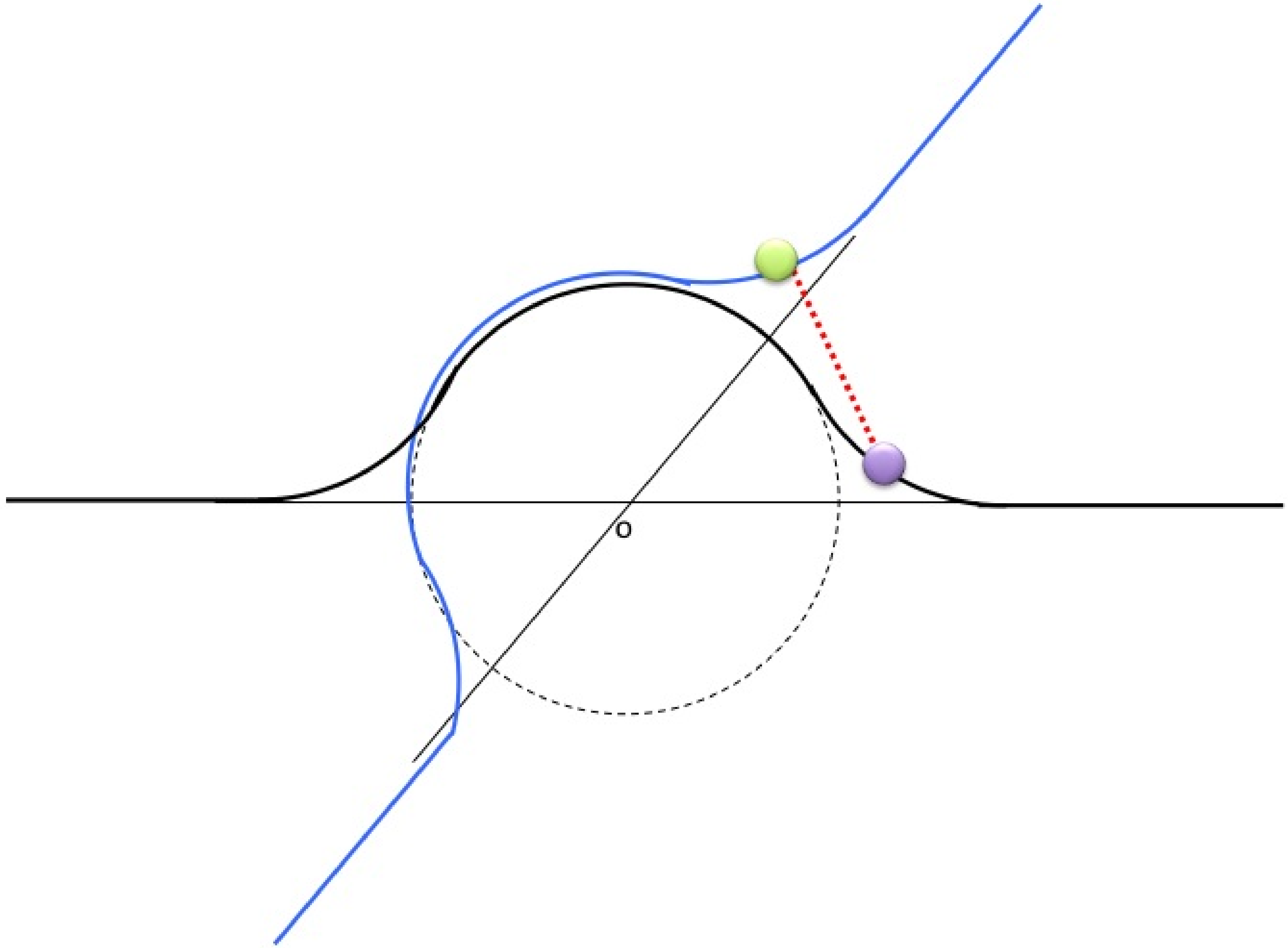
- Both aircrafts continue to fly at the same speed during the maneuver

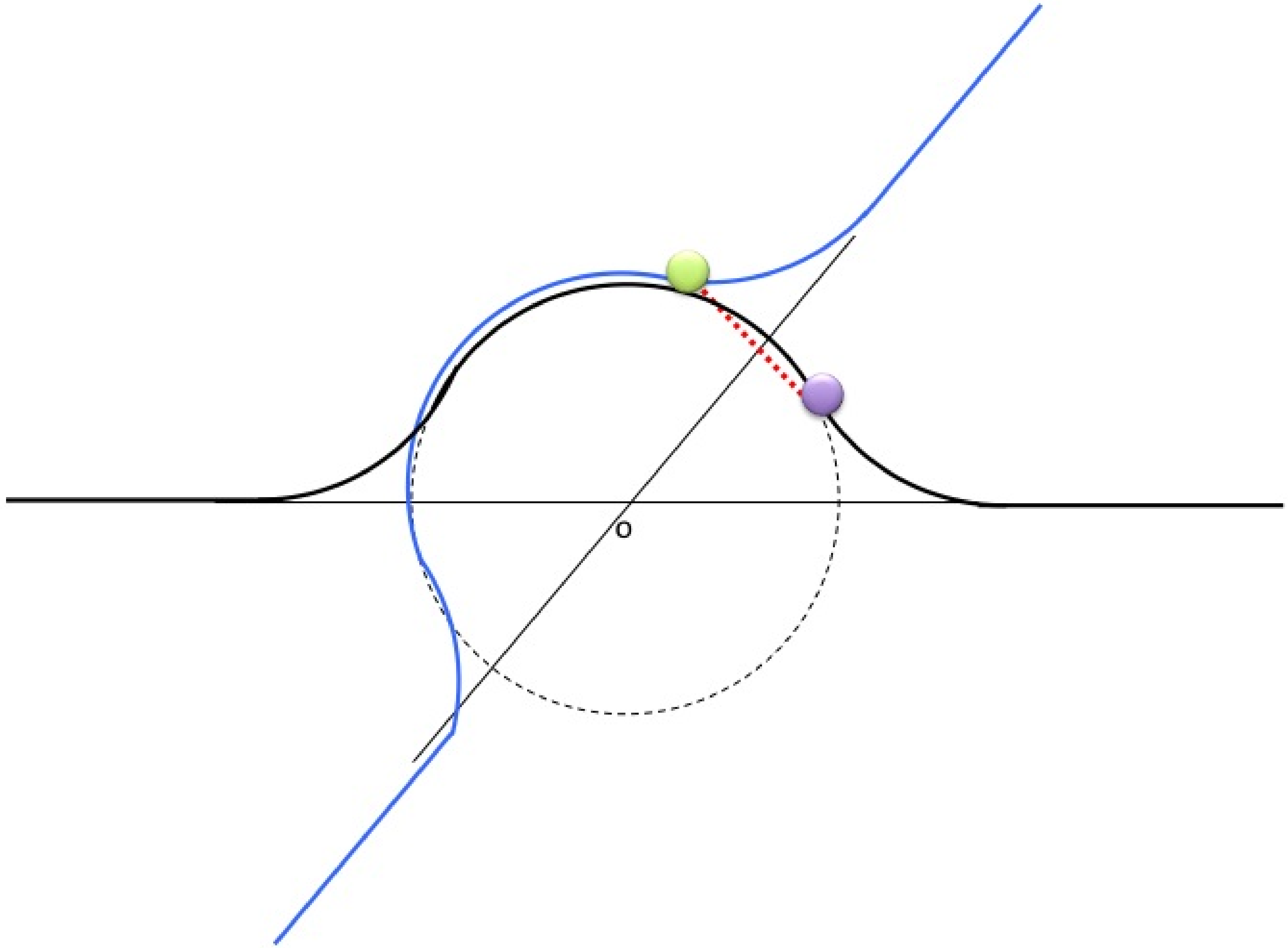

O

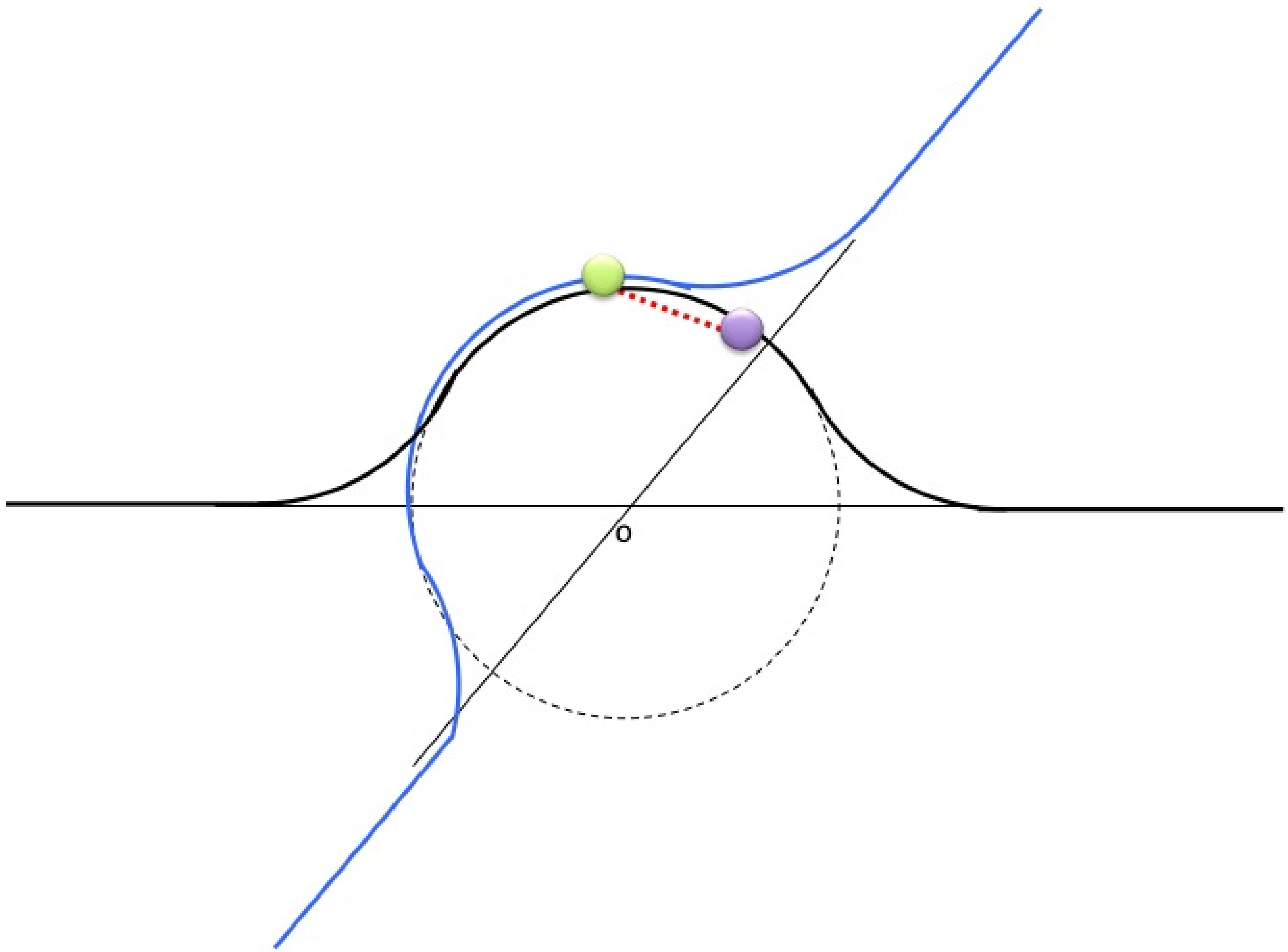

O

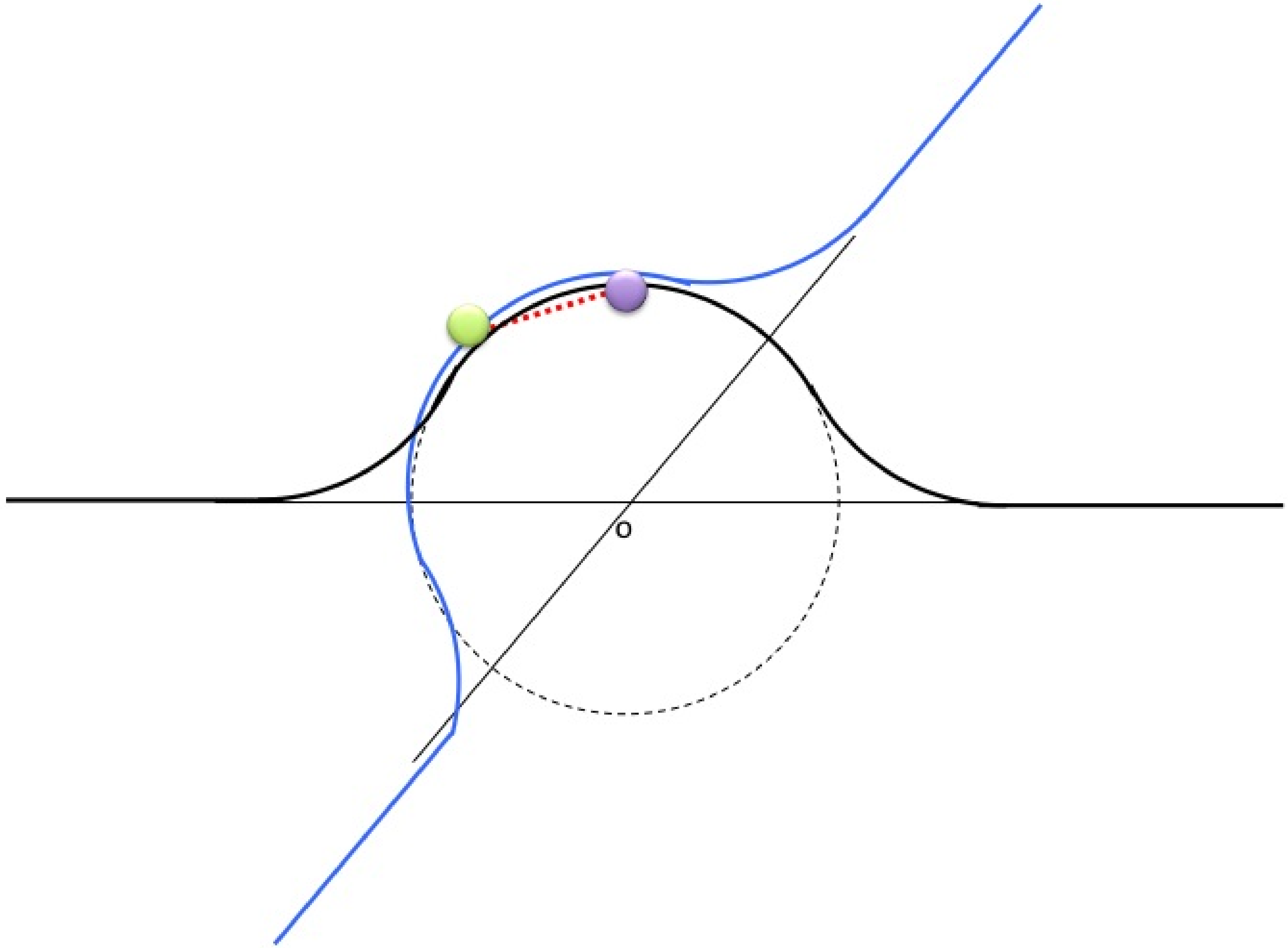

O

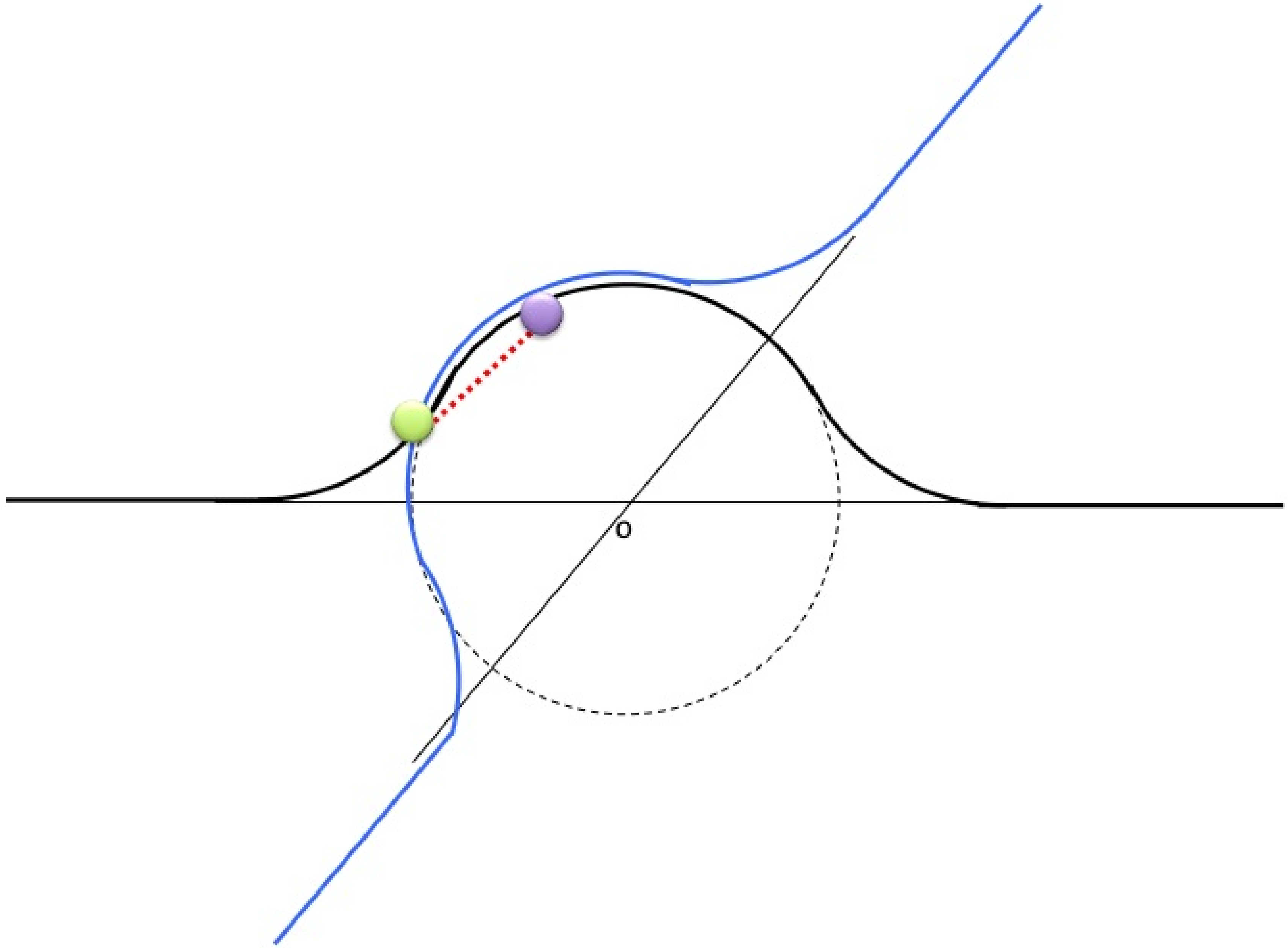

O

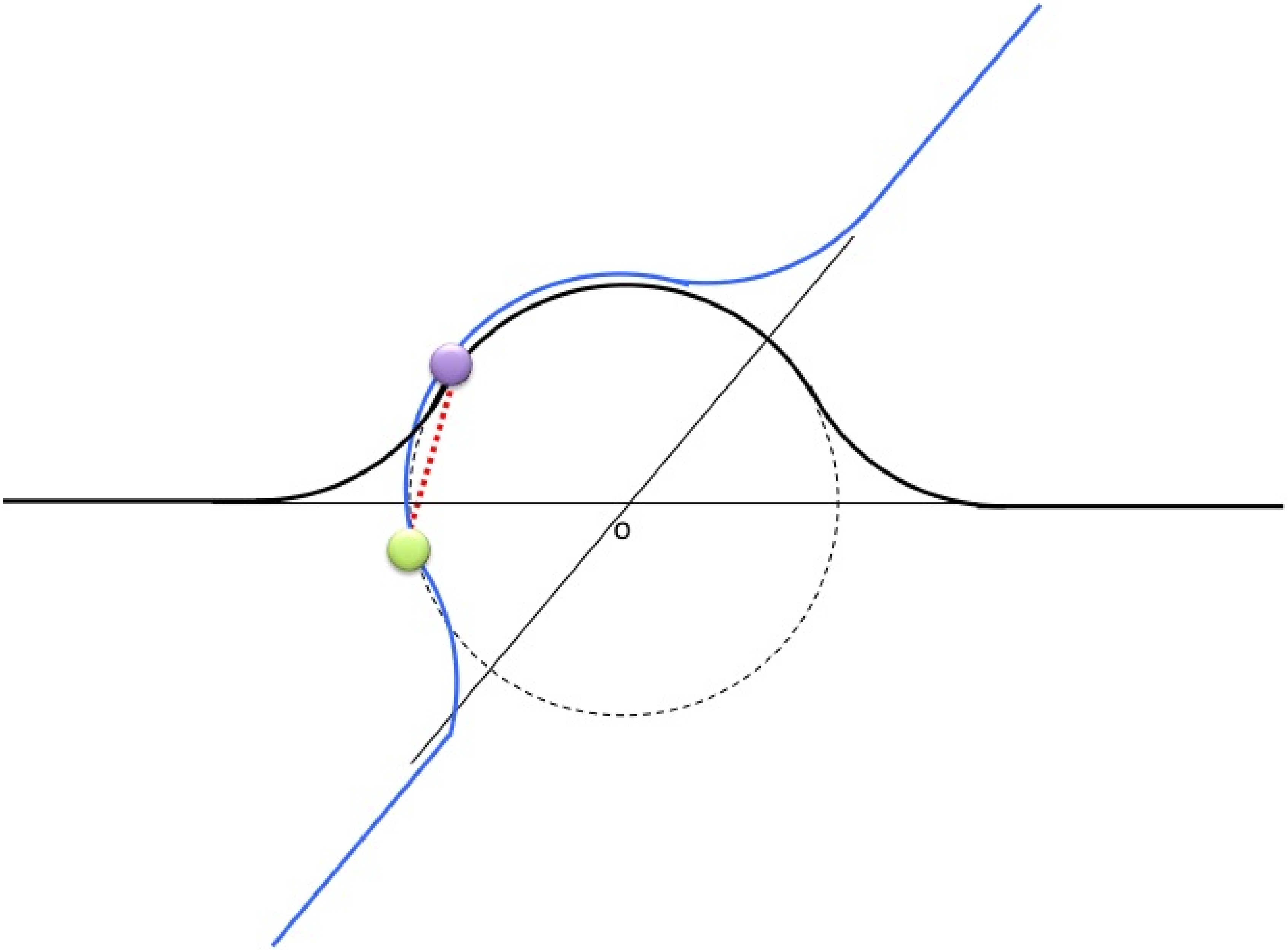

O

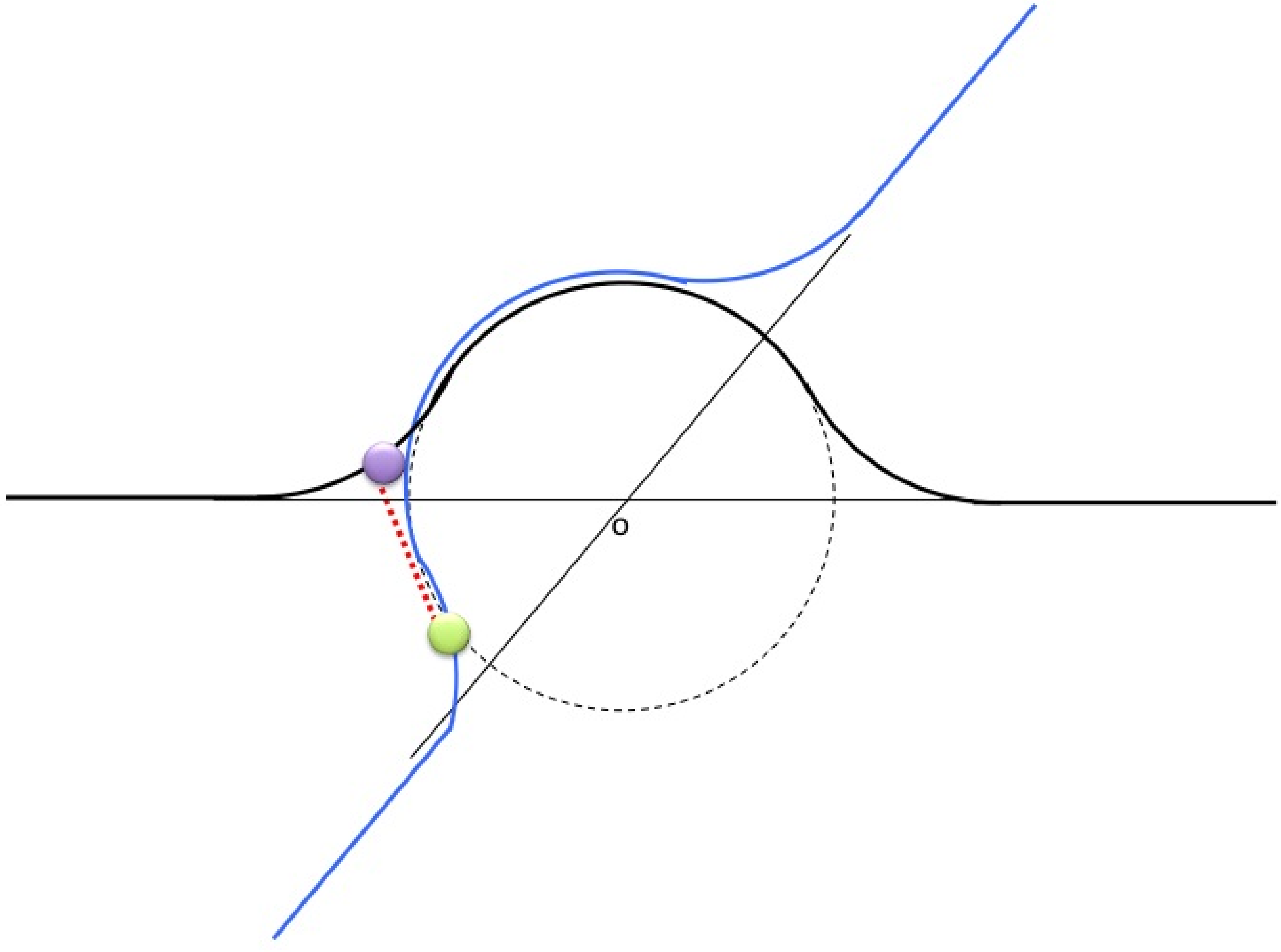

O

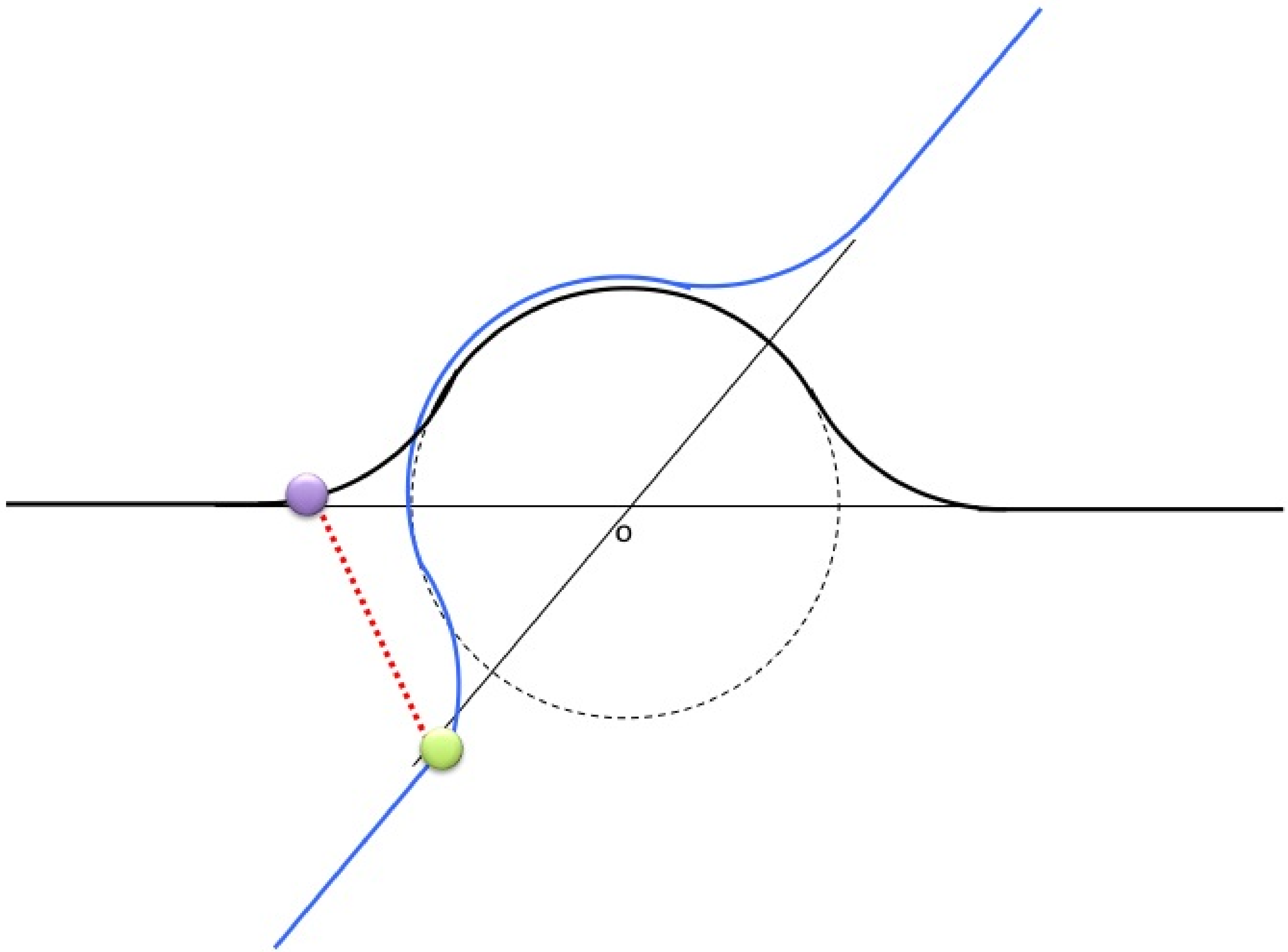

O

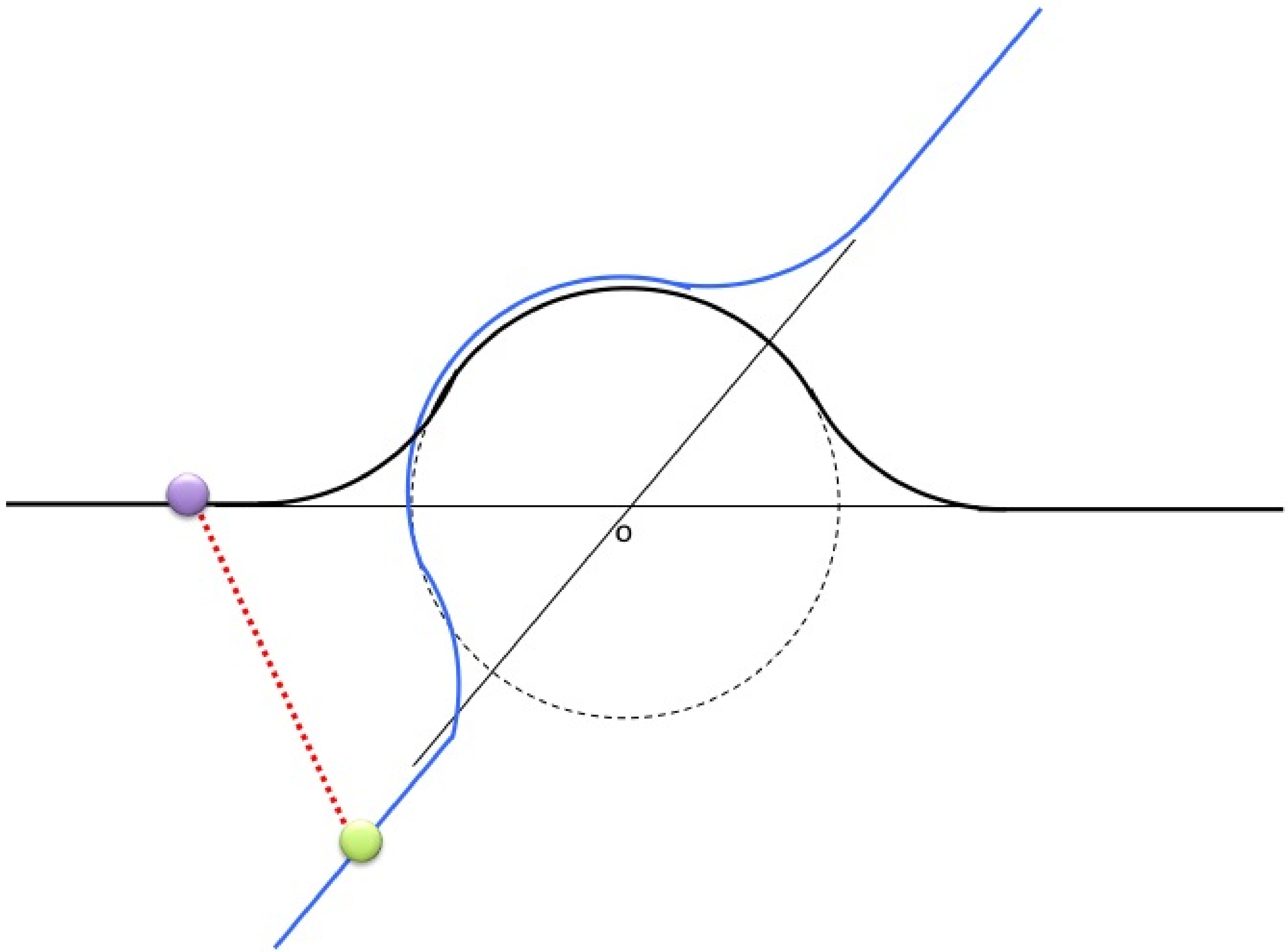

O

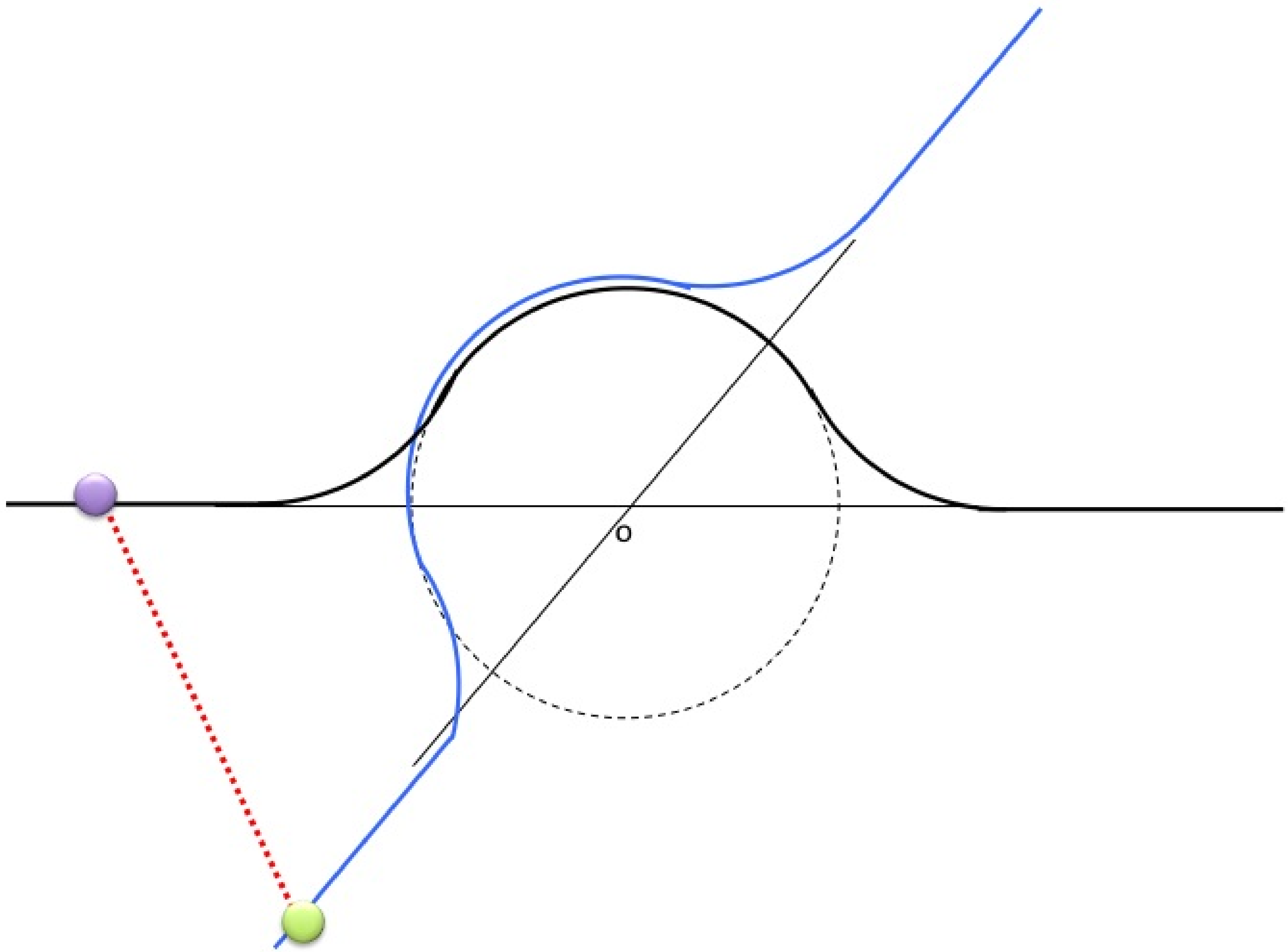

O


O


O


O


O


O

Consequence of the Solution

- Angle ϕ between aircrafts does not change during the maneuver

Consequence of the Solution

- Angle ϕ between aircrafts does not change during the maneuver

- Both aircrafts are still at the same distance rho of the point o

Consequence of the Solution

- Angle ϕ between aircrafts does not change during the maneuver

- Both aircrafts are still at the same distance rho of the point o

- The only parameter that counts then in order to maintain the distance $d \geq p$:

$$d \;=\; 2\rho\sin\frac{\phi}{2} \geq p$$

- Angle ϕ between aircrafts does not change during the maneuver

- Both aircrafts are still at the same distance rho of the point o

- The only parameter that counts then in order to maintain the distance $d \geq p$:

$$d \; = \; 2\rho \sin \frac{\phi}{2} \geq p$$

- is the common distance ρ of both aircrafts to the collision point o

- Angle ϕ between aircrafts does not change during the maneuver

- Both aircrafts are still at the same distance rho of the point o

- The only parameter that counts then in order to maintain the distance $d \geq p$:

$$d \; = \; 2\rho \sin \frac{\phi}{2} \geq p$$

- is the common distance ρ of both aircrafts to the collision point o

- The smallest distance is when they are on the circle (more later)

- Angle ϕ between aircrafts does not change during the maneuver

- Both aircrafts are still at the same distance rho of the point o

- The only parameter that counts then in order to maintain the distance $d \geq p$:

$$d \;=\; 2\rho \sin\frac{\phi}{2} \geq p$$

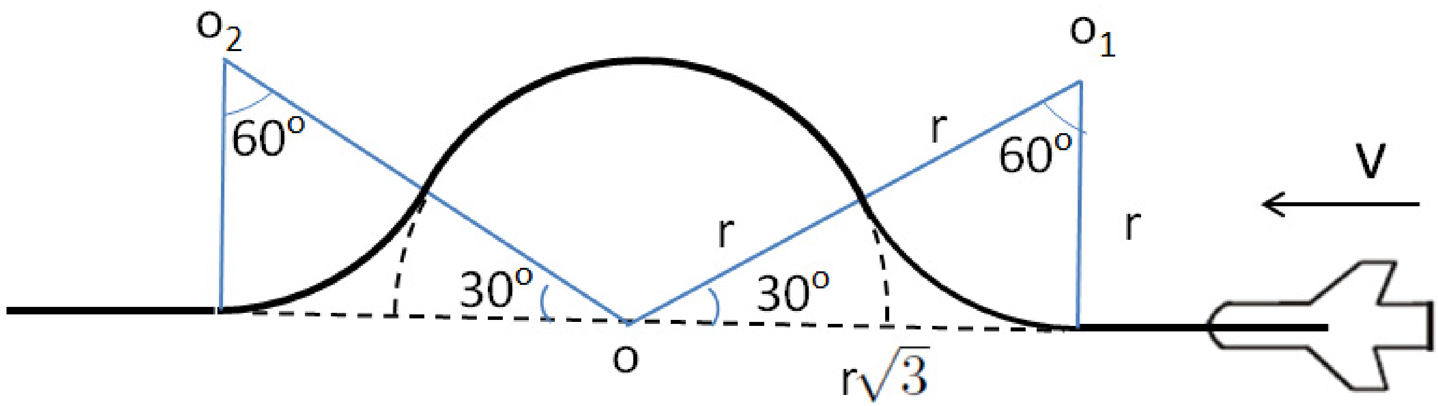
- is the common distance ρ of both aircrafts to the collision point o

- The smallest distance is when they are on the circle (more later)

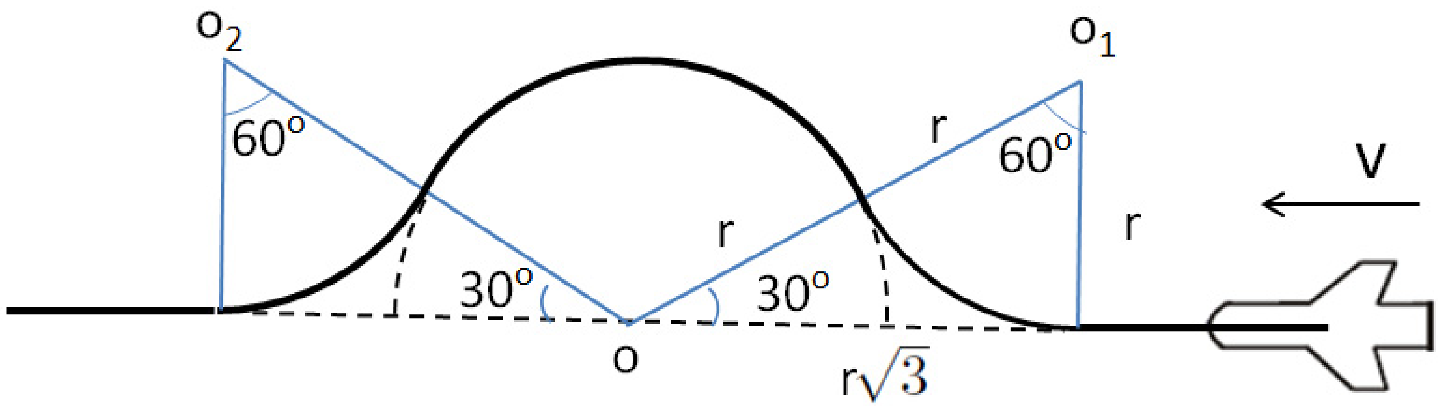
- We must have then: $\frac{p}{2\sin\frac{\phi}{2}} \leq r$

Making the Maneuver more Precise

Making the Maneuver more Precise

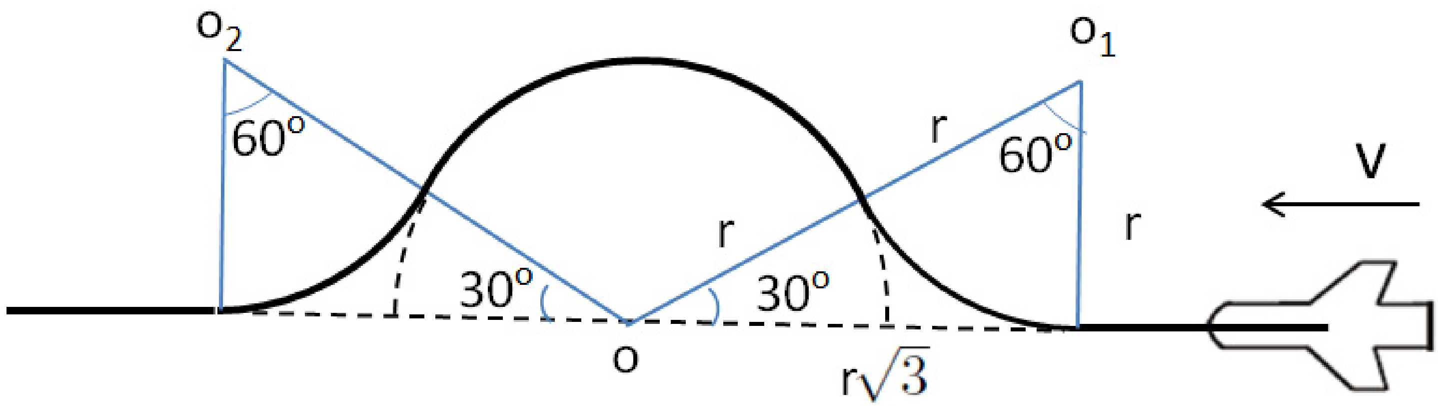


Making the Maneuver more Precise



- Both aircrafts fly as indicated on this figure

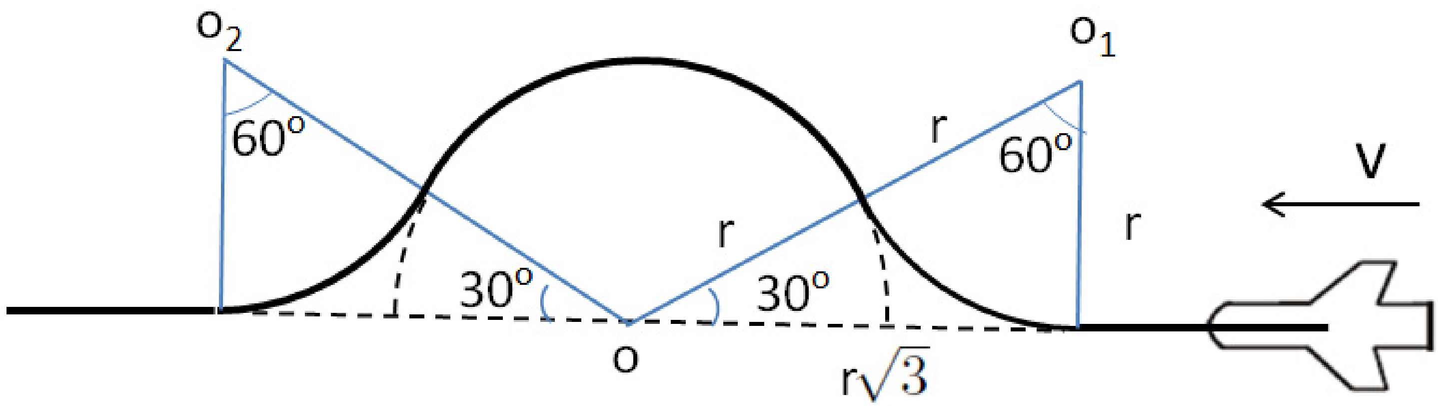
Making the Maneuver more Precise



- Both aircrafts fly as indicated on this figure

- They start the maneuver when at a distance $r\sqrt{3}$ from the point o

Making the Maneuver more Precise

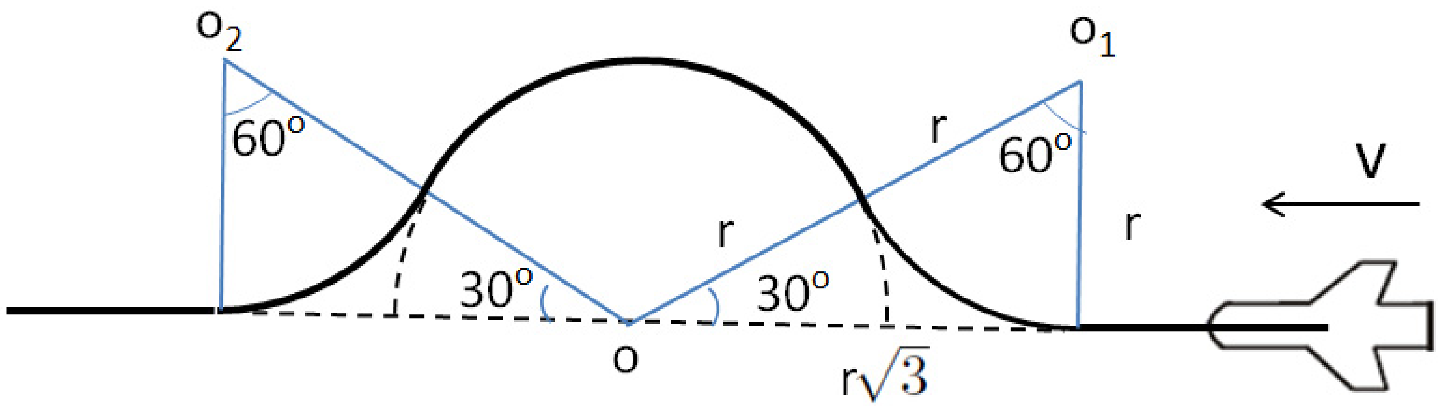


- Both aircrafts fly as indicated on this figure

- They start the maneuver when at a distance $\boldsymbol{r\sqrt{3}}$ from the point $\boldsymbol{o}$

- The airrafts decide to maneuver while at a distance $\boldsymbol{\rho_i}$ from $\boldsymbol{o}$

Making the Maneuver more Precise

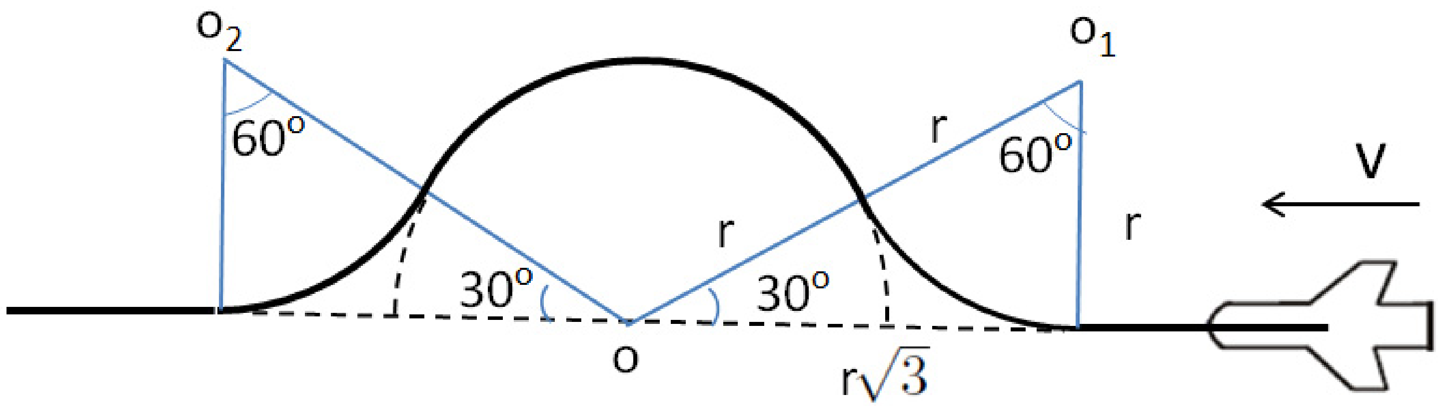


- Both aircrafts fly as indicated on this figure

- They start the maneuver when at a distance $\boldsymbol{r\sqrt{3}}$ from the point $\boldsymbol{o}$

- The airrafts decide to maneuver while at a distance $\boldsymbol{\rho_i}$ from $\boldsymbol{o}$

- We must have then: $\boldsymbol{\rho_i \geq r\sqrt{3}}$ that is $\boldsymbol{r \leq \frac{\rho_i}{\sqrt{3}}}$



- Both aircrafts fly as indicated on this figure

- They start the maneuver when at a distance $r\sqrt{3}$ from the point o

- The airrafts decide to maneuver while at a distance ρ_i from o

- We must have then: $\rho_i \geq r\sqrt{3}$ that is $r \leq \frac{\rho_i}{\sqrt{3}}$

- We have then:

$$\frac{p}{2\sin\frac{\phi}{2}} \leq r \leq \frac{\rho_i}{\sqrt{3}}$$

- Here is again the possible interval for the radius r of the circle:

$$\frac{p}{2\sin\frac{\phi}{2}} \leq r \leq \frac{\rho_i}{\sqrt{3}}$$

- We must have then the following for the constants ρ_i, ϕ, and p:

$$2\rho_i \sin\frac{\phi}{2} \geq p\sqrt{3}$$

- ϕ is the angle of the two trajectories

- ρ_i is the initial distance of the two aircrafts to the collision point o

- p is the minimal safety distance between the two aircrafts

axm1: $\phi \in 0 \,..\, \pi$

axm2: $\rho_i \in \mathbb{R}^+$

axm2: $p \in \mathbb{R}^+$

axm4: $2\rho_i \sin\frac{\phi}{2} \geq p\sqrt{3}$

- In this initial model, we are still discrete

- $phase$ corresponds to the various discrete events
- ρ is the common distance of the aircrafts to the collision point o
- r is the circle radius

inv1: $phase \in \{0, 1, 2, 3, 4, 5\}$

inv2: $\rho \in \mathbb{R}^+$

inv3: $r \in \mathbb{R}^+$

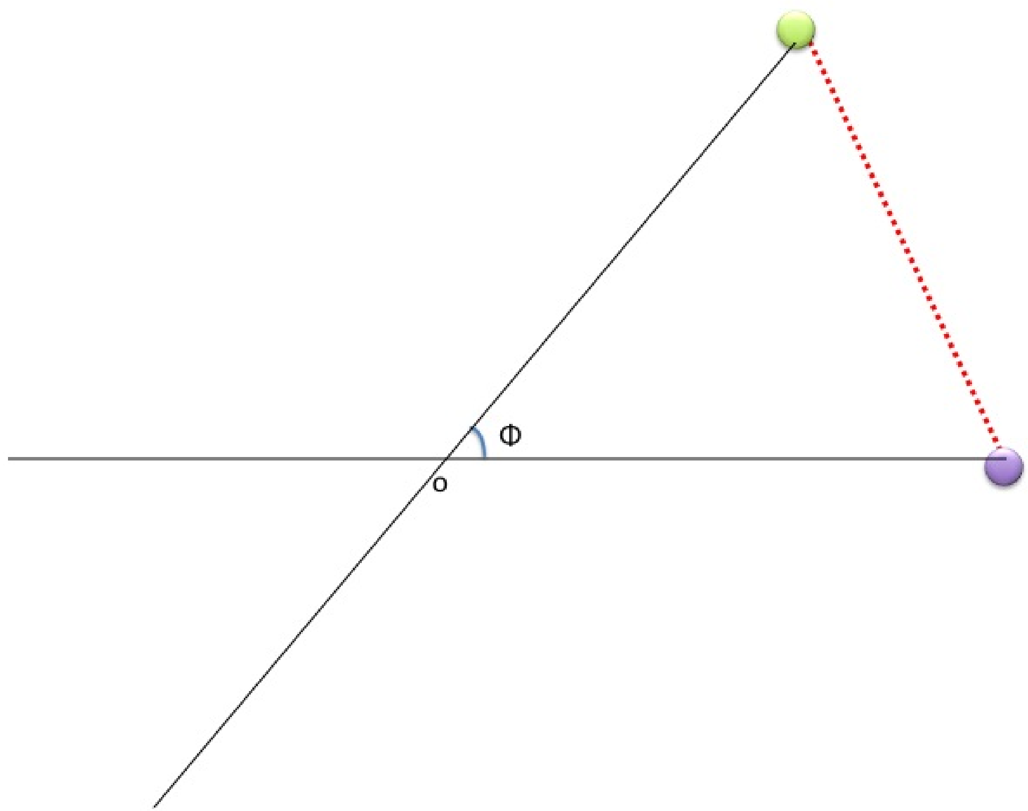
inv4: $2\rho \sin \frac{\phi}{2} \geq p$

- **inv4** is the safety invariant: the minimal authorized distance is p

The Various Discrete Events

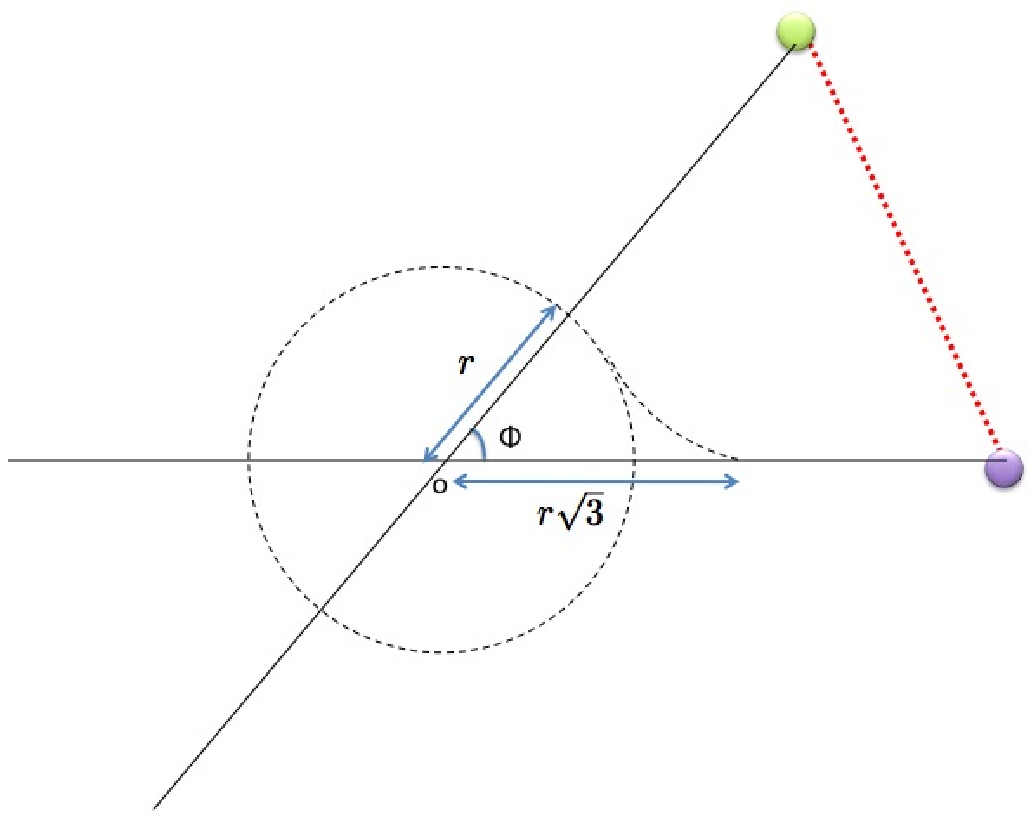
- INIT: initialisation
- agree: choose the radius of the circle
- start: start the maneuver
- enter: entering the circle
- cycle: move on the circle
- leave: leaving the circle

INIT
begin
$\rho := \rho_i$
$phase := 0$
$r :\in \mathbb{R}^+$
end



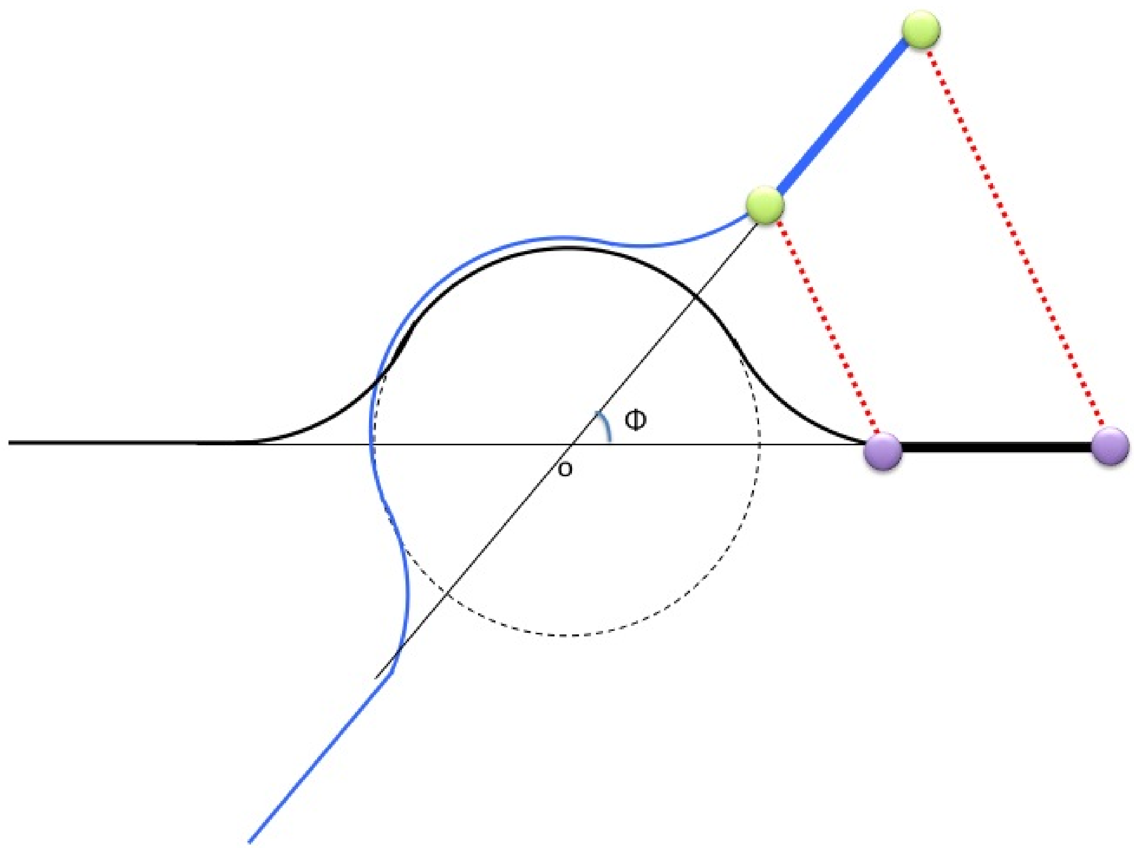
```
agree
  any c where
    phase = 0
    p ≤ 2c sin φ/2
    c√3 ≤ ρ_i
  then
    phase := 1
    r := c
  end
```

Choosing the radius r of the circle



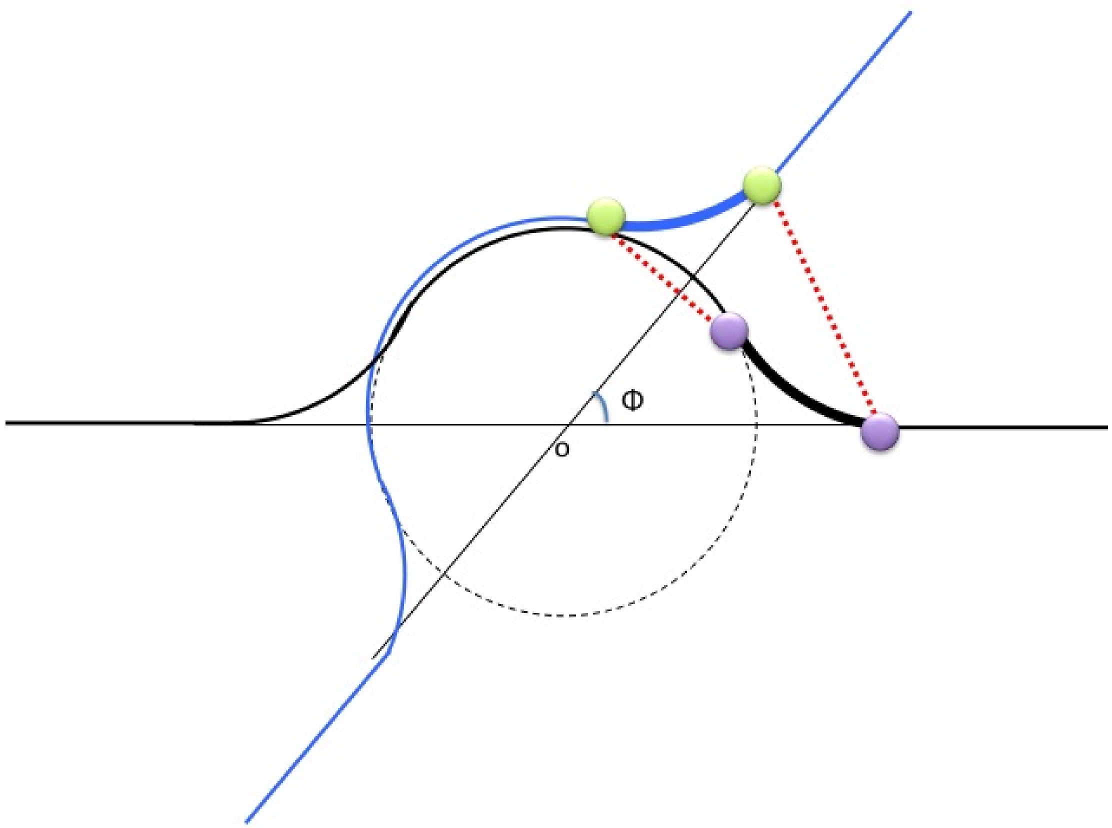
start
when
$phase = 1$
then
$phase := 2$
$\rho := r\sqrt{3}$
end

ρ goes from ρ_i to $r\sqrt{3}$



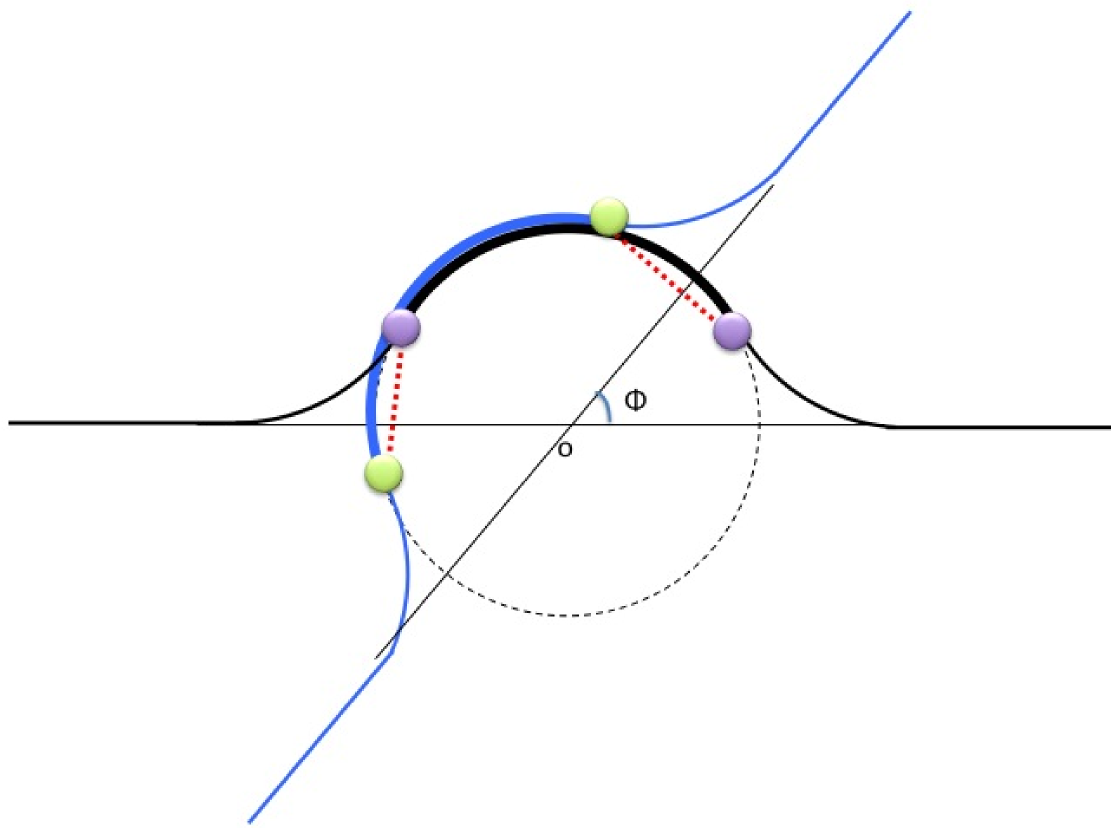
enter
when
$\quad phase = 2$
then
$\quad phase := 3$
$\quad \rho := r$
end

ρ goes from $r\sqrt{3}$ to r



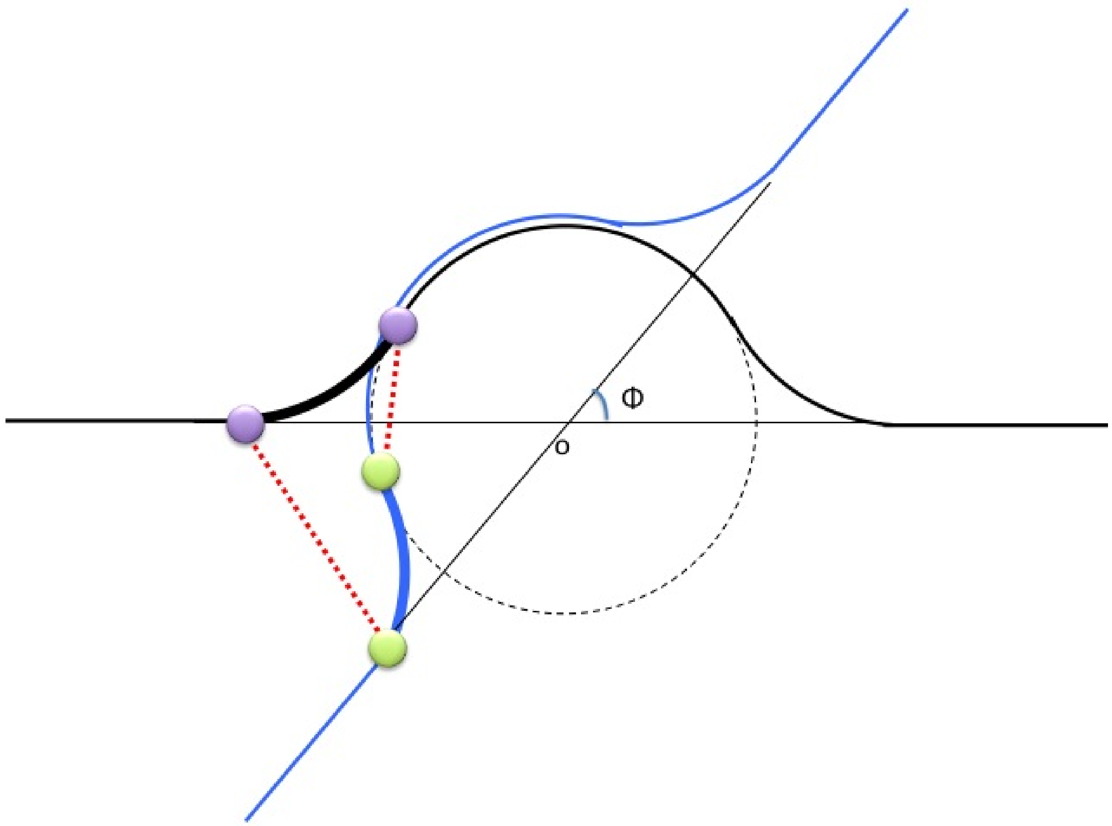
cycle
when
$phase = 3$
then
$phase := 4$
$\rho := r$
end

ρ goes from r to r



leave
when
  $phase = 4$
then
  $phase := 5$
  $\rho := r\sqrt{3}$
end

ρ goes from r to $r\sqrt{3}$



- We introduce the intermediate continuous parts

- We replace ρ by ρ_c (that is $\rho\_continuous$)

- We introduce now, the present time

$$
\begin{array}{ll}
\textbf{inv1\_1:} & \rho\_c \in \mathbb{R}^{+} \rightarrow\!\!\!\!\!\!+ \mathbb{R} \\
\textbf{inv1\_2:} & now \in \mathrm{dom}(\rho\_c) \\
\textbf{inv1\_3:} & \rho = \rho\_c(now) \\
\textbf{inv1\_4:} & \forall t \cdot t \in \mathrm{dom}(\rho\_c) \;\Rightarrow\; 2\rho\_c(t)\sin\frac{\phi}{2} \geq p
\end{array}
$$

- **inv1_3** is the gluing invariant

- **inv1_4** generalises the previous invariant: $2\rho\sin\frac{\phi}{2} \geq p$

(abstract-)INIT

begin

$\rho := \rho_i$

$phase := 0$

$r :\in \mathbb{R}^+$

end

(concrete-)INIT

begin

$\rho\_c := \{0 \mapsto \rho_i\}$

$phase := 0$

$r :\in \mathbb{R}^+$

$now := 0$

end

agree

any c **where**

$phase = 0$

$p \leq 2c \sin \frac{\phi}{2}$

$c\sqrt{3} \leq \rho_i$

then

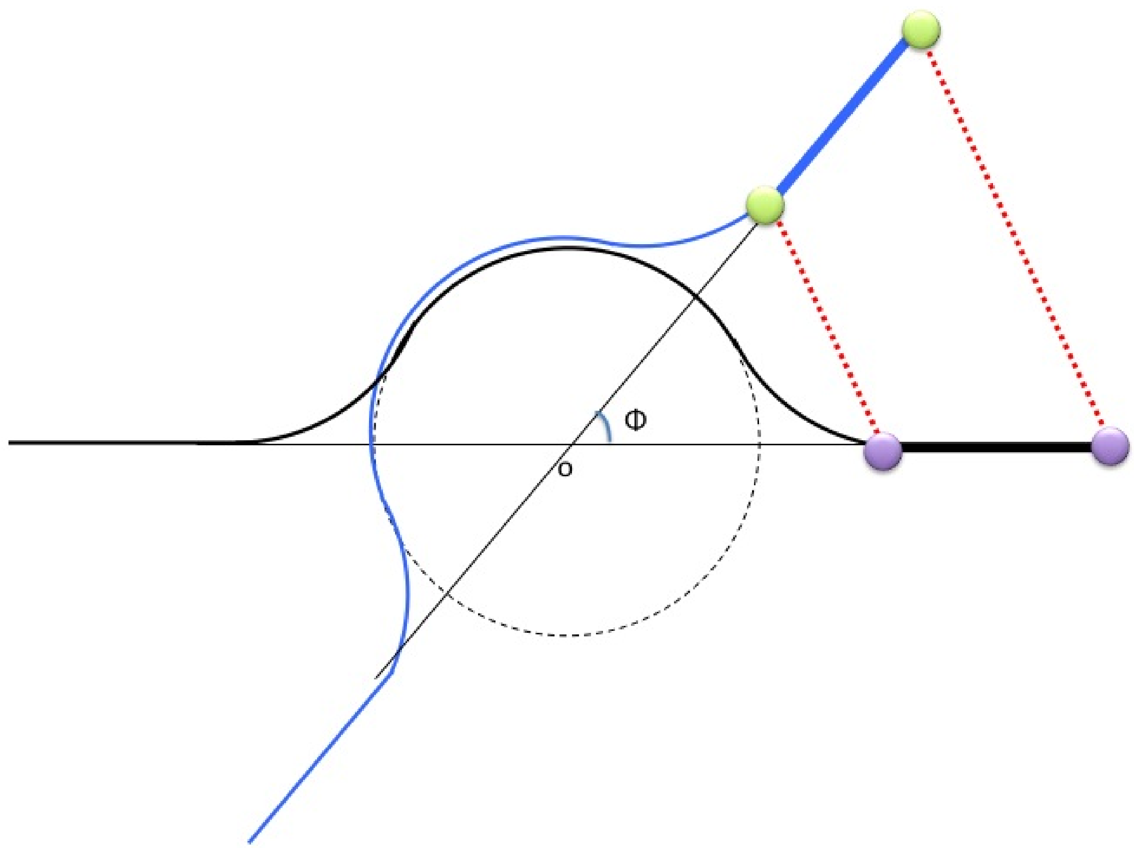
$phase := 1$

$r := c$

end

(abstract-)start
when
$phase = 1$
then
$phase := 2$
$\rho := r\sqrt{3}$
end

(concrete-)start
when
$phase = 1$
then
$phase := 2$
$\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{(\rho_i - r\sqrt{3})}{v} \mid \rho_i - v(t - now)$
$now := now + \frac{(\rho_i - r\sqrt{3})}{v}$
end

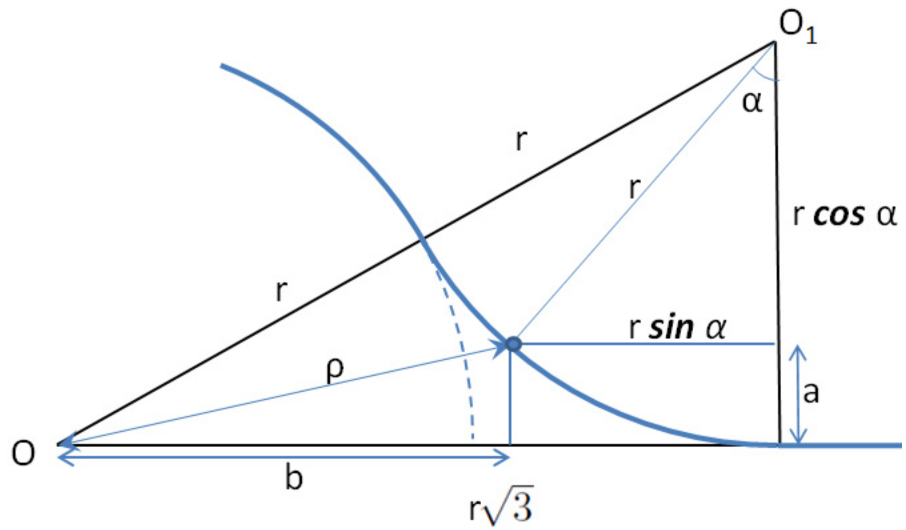


More on the start event

start
  when
    $phase = 1$
  then
    $phase := 2$
    $\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{(\rho_i - r\sqrt{3})}{v} \mid \rho_i - v(t - now)$
    $now := now + \frac{(\rho_i - r\sqrt{3})}{v}$
  end

- $\rho\_c(now) = \rho_i$
- $\rho\_c(now + \frac{(\rho_i - r\sqrt{3})}{v}) = r\sqrt{3}$
- ρ_c decreases linearly from ρ_i to $r\sqrt{3}$
- $\frac{(\rho_i - r\sqrt{3})}{v}$ is the time it takes to fly from ρ_i to $r\sqrt{3}$

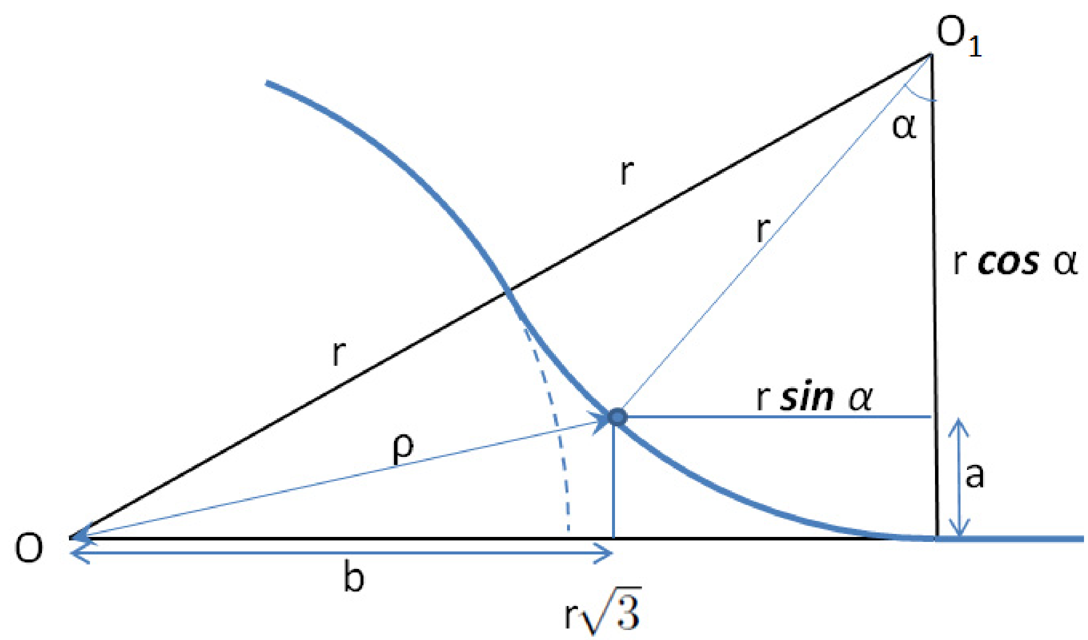
Computing ρ During First Part of Maneuver



$$\rho^2 = a^2 + b^2$$
$$= r^2(1 - \cos\alpha)^2 + r^2(\sqrt{3} - \sin\alpha)^2$$
$$= r^2(5 - 4\cos(\tfrac{\pi}{3} - \alpha))$$
$$\rho = r\sqrt{5 - 4\cos(\tfrac{\pi}{3} - \alpha)}$$

- ρ decreases from $r\sqrt{3}$ to r when α goes from 0 to $\frac{\pi}{3}$.

Computing ρ During First Part of Maneuver



- The angle α increases from 0 to $\frac{\pi}{3}$ during this phase

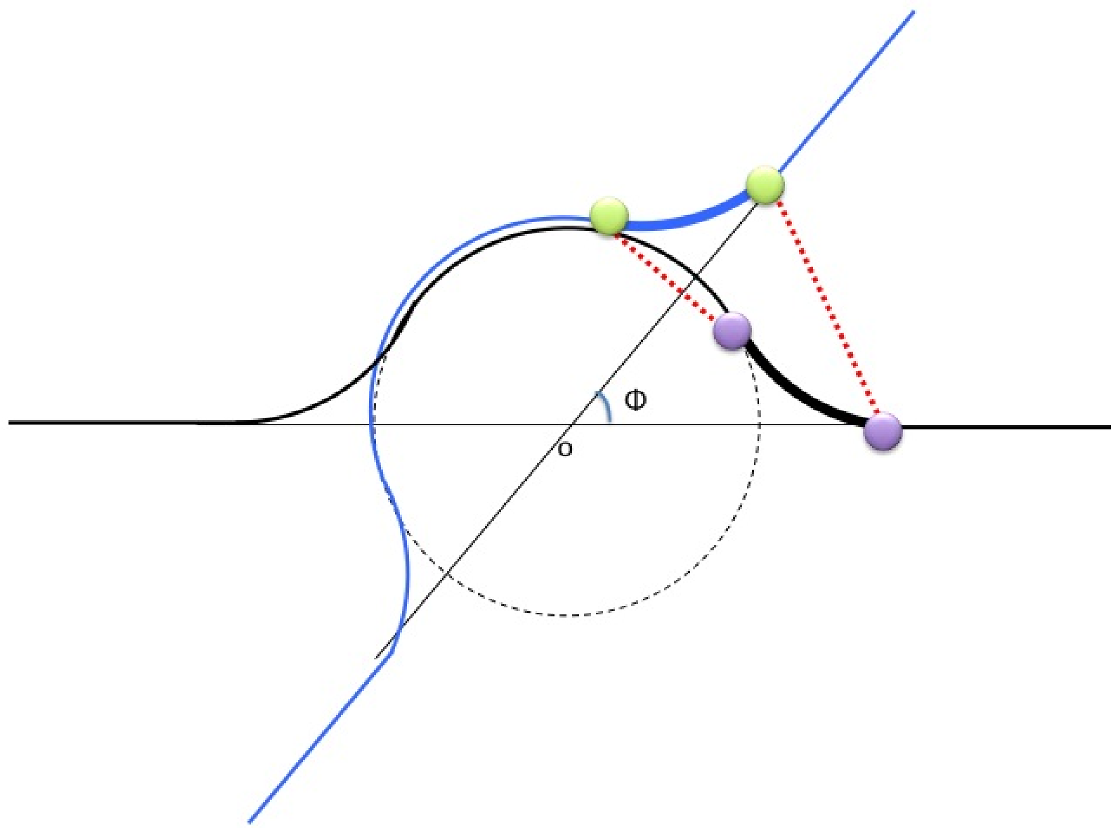
- The distance is $\frac{\pi r}{3}$

- The time to cover this distance is thus $\frac{\pi r}{3v}$

- We have: $\alpha \ = \ \frac{v(t-now)}{r}$

(abstract-)enter
when
$phase = 2$
then
$phase := 3$
$\rho := r$
end

(concrete-)enter
when
$phase = 2$
then
$phase := 3$
$\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{\pi r}{3v} \mid r\sqrt{5 - 4\cos(\frac{\pi}{3} - \frac{v(t-now)}{r})}$
$now := now + \frac{\pi r}{3v}$
end



enter
when
$phase = 2$
then
$phase := 3$
$\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{\pi r}{3v} \mid r\sqrt{5 - 4\cos(\frac{\pi}{3} - \frac{v(t-now)}{r})}$
$now := now + \frac{\pi r}{3v}$
end

- $\rho\_c(now) \;=\; r\sqrt{5 - 4\cos\frac{\pi}{3}} \;=\; r\sqrt{5 - \frac{4}{2}} \;=\; r\sqrt{3}$
- $\rho\_c(now + \frac{\pi r}{3v}) \;=\; r\sqrt{5 - 4\cos(\frac{\pi}{3} - \frac{v\pi r}{r3v})} \;=\; r\sqrt{5 - 4\cos 0} \;=\; r$
- ρ_c decreases non-linearly from $r\sqrt{3}$ to r

Derivation of $\rho\_c(t)$

$$\rho\_c(t) = r\sqrt{5 - 4\cos(\frac{\pi}{3} - \frac{v(t - now)}{r})}$$

Thus

$$\frac{d\rho\_c(t)}{dt} = \frac{4r\sin(\frac{\pi}{3} - \frac{v(t-now)}{r})}{2\sqrt{5 - 4\cos(\frac{\pi}{3} - \frac{v(t-now)}{r})}} \frac{-v}{r}$$

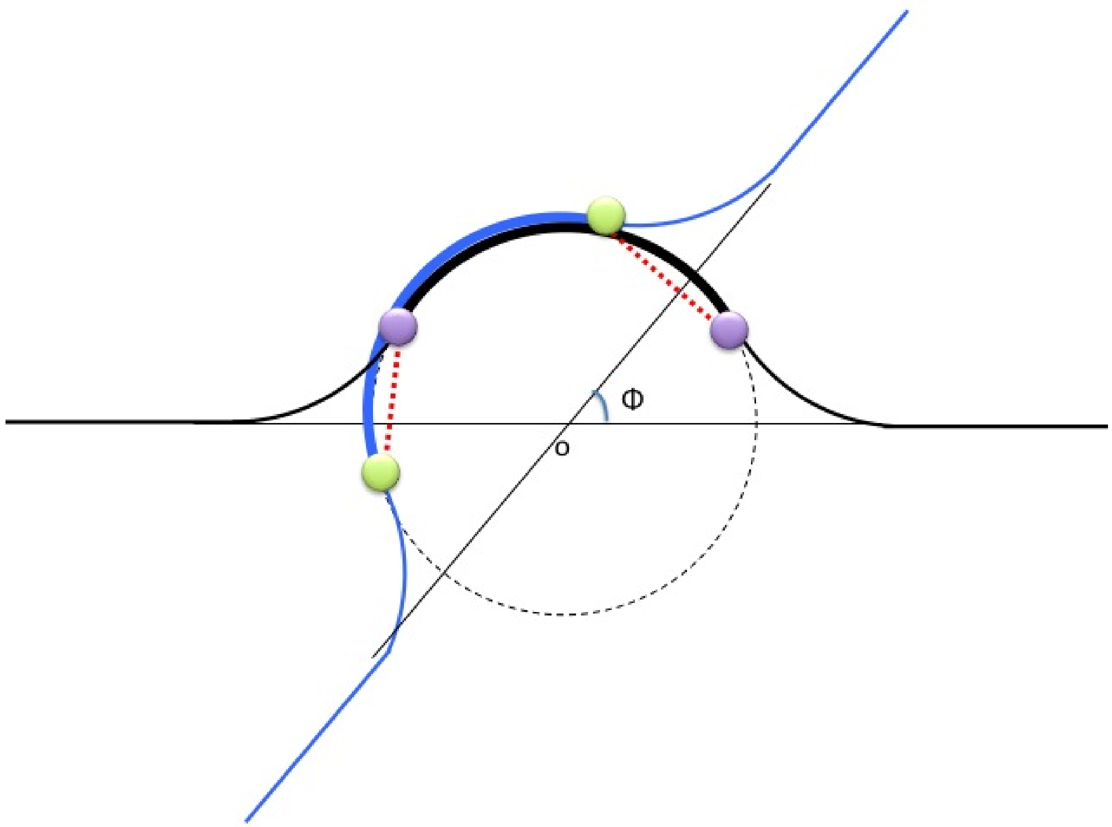
When t increases from now to $now + \frac{\pi r}{3v}$, then the derivative $\frac{d\rho\_c(t)}{dt}$ increases monotonically from $-v$ to 0:

$$\frac{d\rho\_c(t)}{dt}_{t=now} = -v$$

$$\frac{d\rho\_c(t)}{dt}_{t=now+\frac{\pi r}{3v}} = 0$$

(abstract-)cycle
when
$phase = 3$
then
$phase := 4$
$\rho := r$
end

(concrete-)cycle
when
$phase = 3$
then
$phase := 4$
$\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{2\pi r}{3v} \mid r$
$now := now + \frac{2\pi r}{3v}$
end



```
cycle
  when
    phase = 3
  then
    phase := 4
    ρ_c := λt·t ∈ now .. now + 2πr/(3v) | r
    now := now + 2πr/(3v)
  end
```

$$\text{cycle}$$
$$\textbf{when}\quad phase = 3$$
$$\textbf{then}\quad phase := 4,\quad \rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{2\pi r}{3v} \mid r,\quad now := now + \frac{2\pi r}{3v}$$
$$\textbf{end}$$

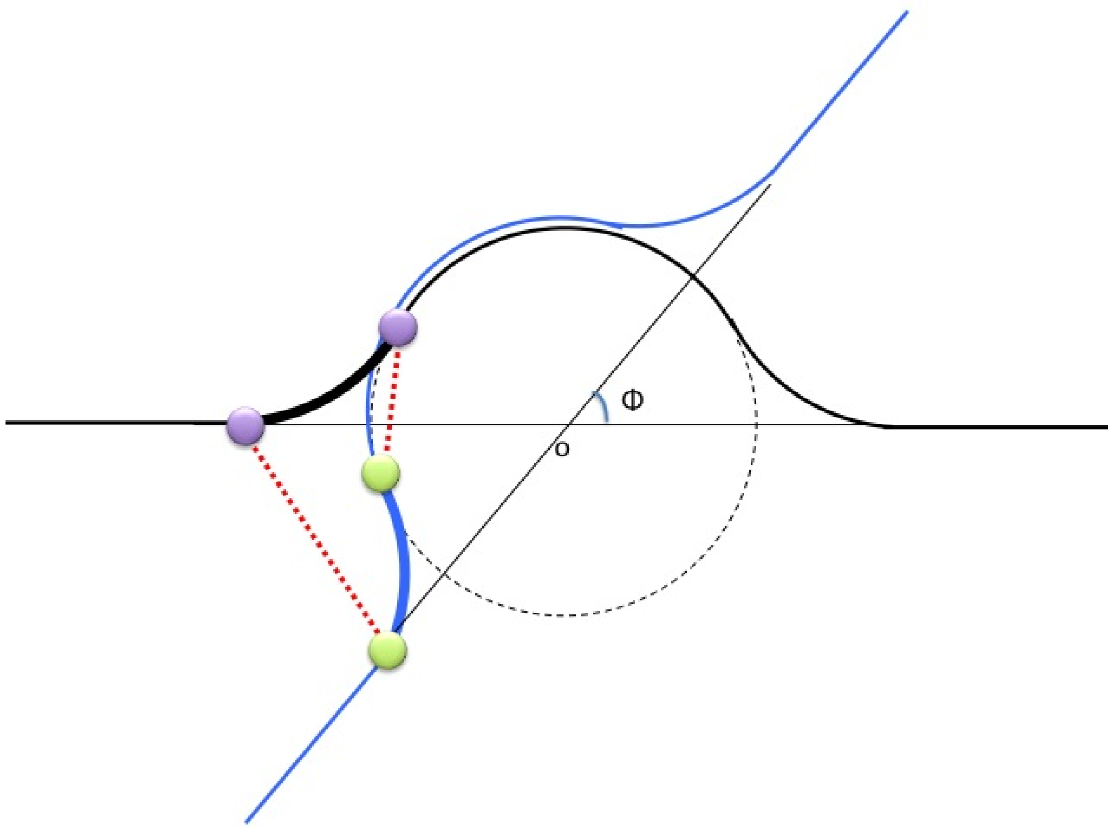
- $\rho\_c(now) \;=\; r$

- $\rho\_c(now + \frac{2\pi r}{3v}) \;=\; r$

- ρ_c remains constant to r

(abstract-)leave
  when
    $phase = 4$
  then
    $phase := 5$
    $\rho := r\sqrt{3}$
  end

(concrete-)leave
  when
    $phase = 4$
  then
    $phase := 5$
    $\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{\pi r}{3v} \mid r\sqrt{5 - 4\cos(\frac{v(t-now)}{r})}$
    $now := now + \frac{\pi r}{3v}$
  end



leave
when
$phase = 4$
then
$phase := 5$
$\rho\_c := \lambda t \cdot t \in now \,..\, now + \frac{\pi r}{3v} \mid r\sqrt{5 - 4\cos(\frac{v(t-now)}{r})}$
$now := now + \frac{\pi r}{3v}$
end

- $\rho\_c(now) \;=\; r\sqrt{5 - 4\cos 0} \;=\; r$
- $\rho\_c(now + \frac{\pi r}{3v}) \;=\; r\sqrt{5 - 4\cos\frac{\pi}{3}} \;=\; r\sqrt{5 - \frac{4}{2}} \;=\; r\sqrt{3}$
- ρ_c increases non-linearly from r to $r\sqrt{3}$

Derivation of $\rho\_c(t)$

$$\rho\_c(t) \;=\; r\sqrt{5 - 4\cos(\frac{v(t-now)}{r})}$$

Thus

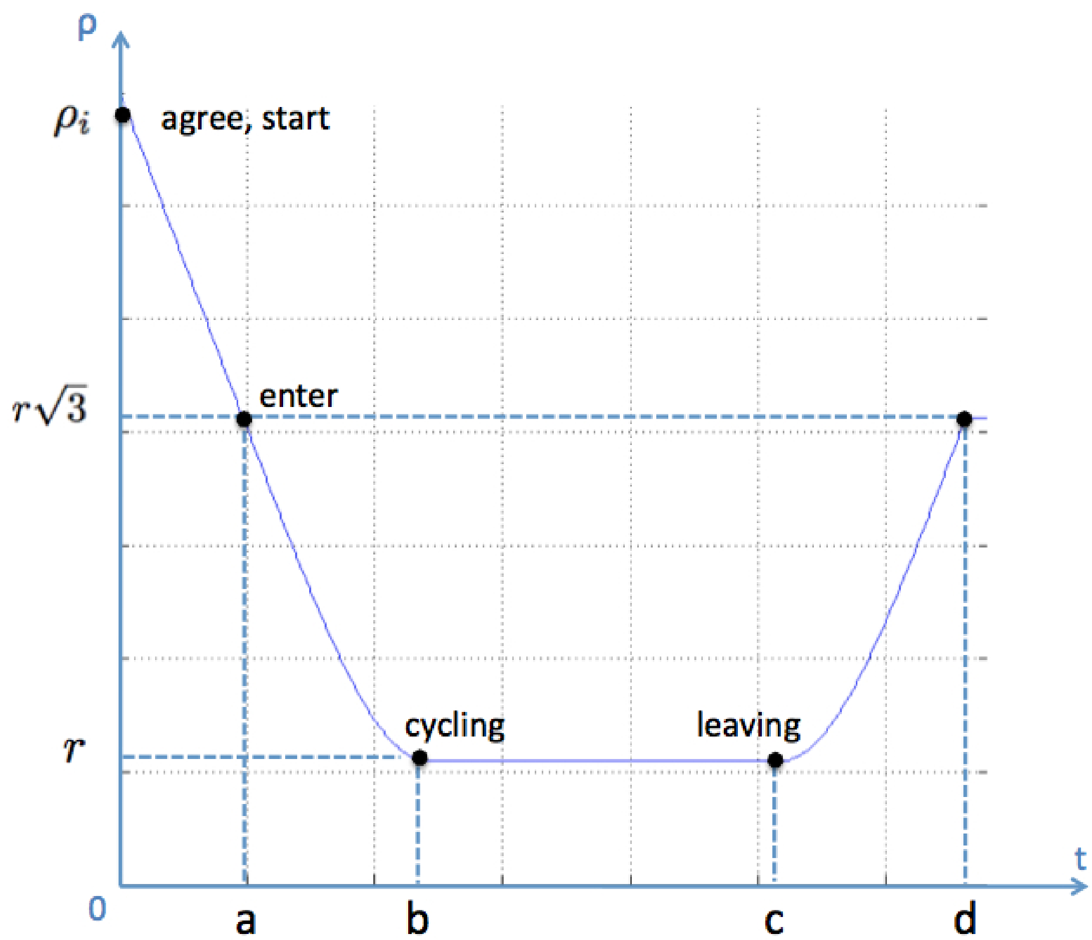
$$\frac{d\rho\_c(t)}{dt} \;=\; \frac{4r\sin(\frac{v(t-now)}{r})}{2\sqrt{5-4\cos(\frac{v(t-now)}{r})}}\frac{v}{r}$$

When t increases from now to $now + \frac{\pi r}{3v}$, then the derivative $\frac{d\rho\_c(t)}{dt}$ increases monotonically from 0 to v:

$$\frac{d\rho\_c(t)}{dt}_{t=now} \;=\; 0$$

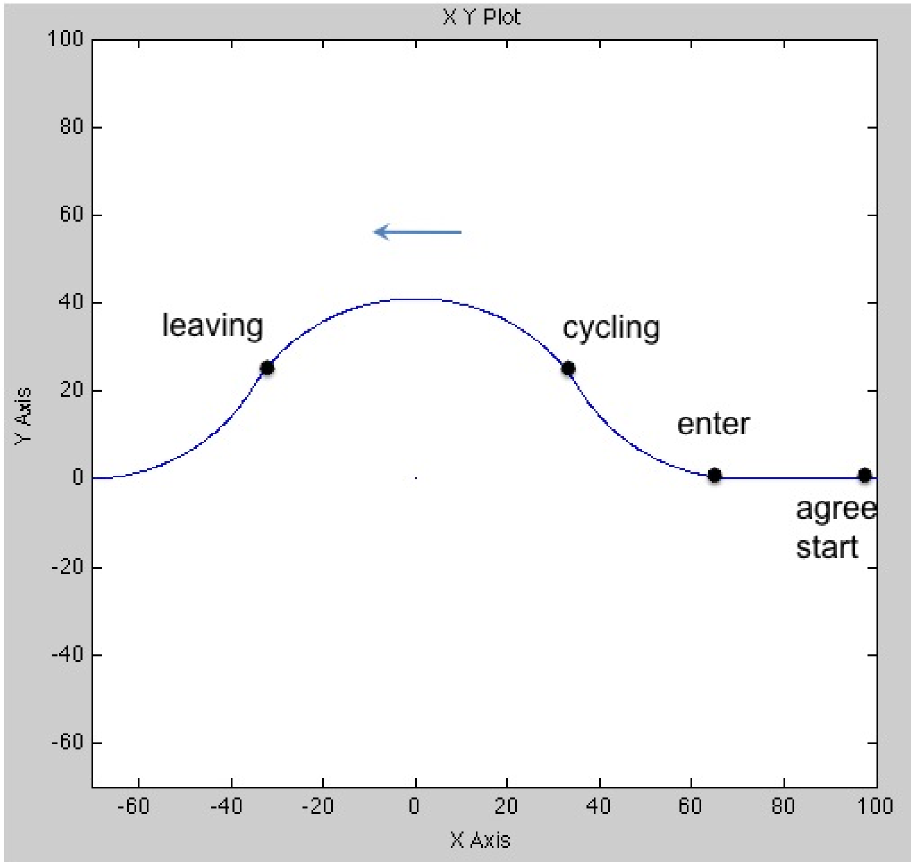
$$\frac{d\rho\_c(t)}{dt}_{t=now+\frac{\pi r}{3v}} \;=\; v$$

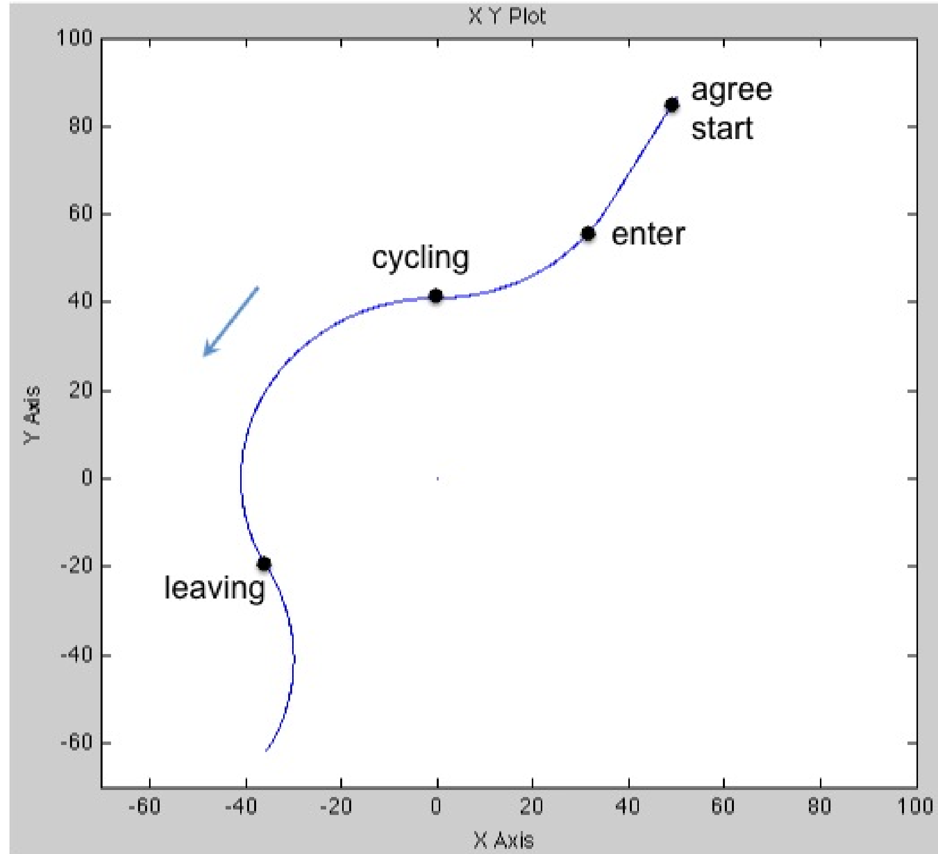
Mathlab/Simulink Output 1: Variation of ρ with Time



$$a = \frac{\rho_i - r\sqrt{3}}{v}, \qquad b = a + \frac{\pi r}{3v}, \qquad c = b + \frac{2\pi r}{3v}, \qquad d = c + \frac{\pi r}{3v}$$

Mathlab/Simulink Output 2: Aircraft Trajectories

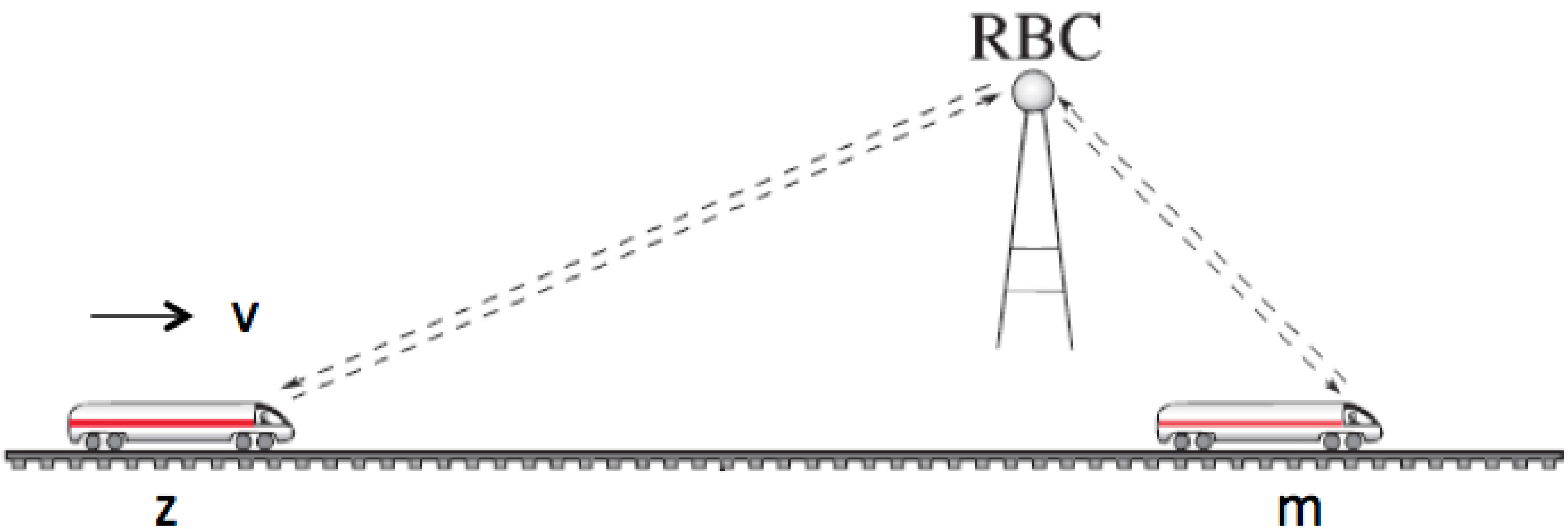




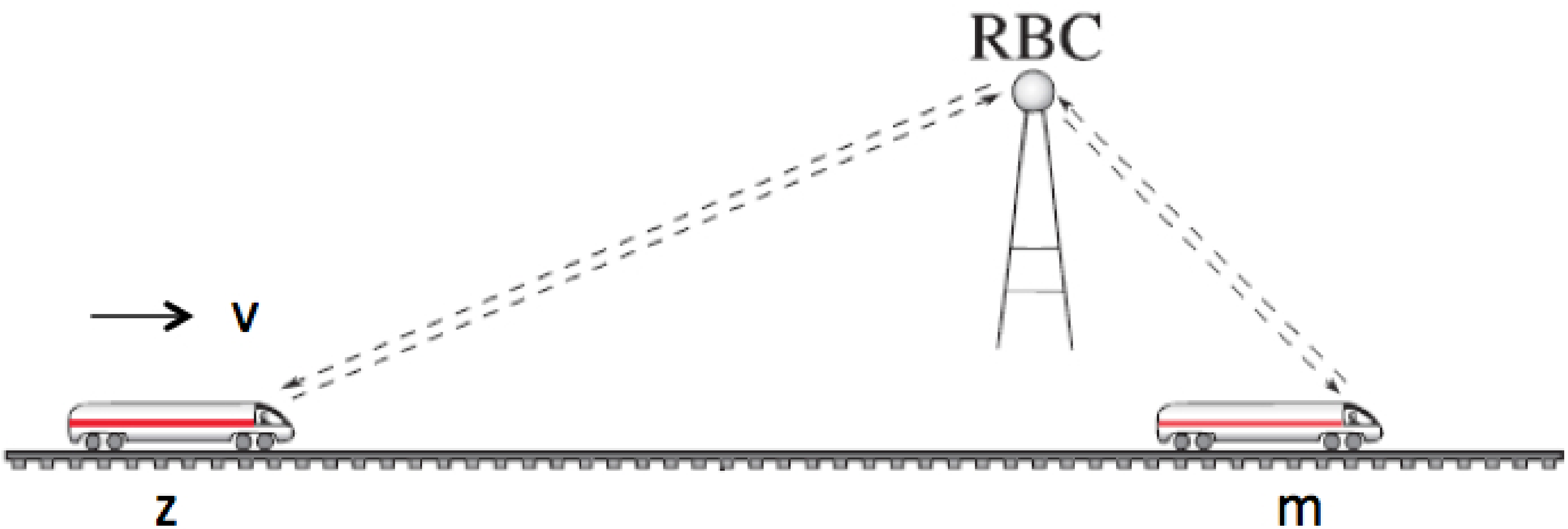
Example 2

- Two trains are sent some information by Radio BroadCasting

- Two trains are sent some information by Radio BroadCasting

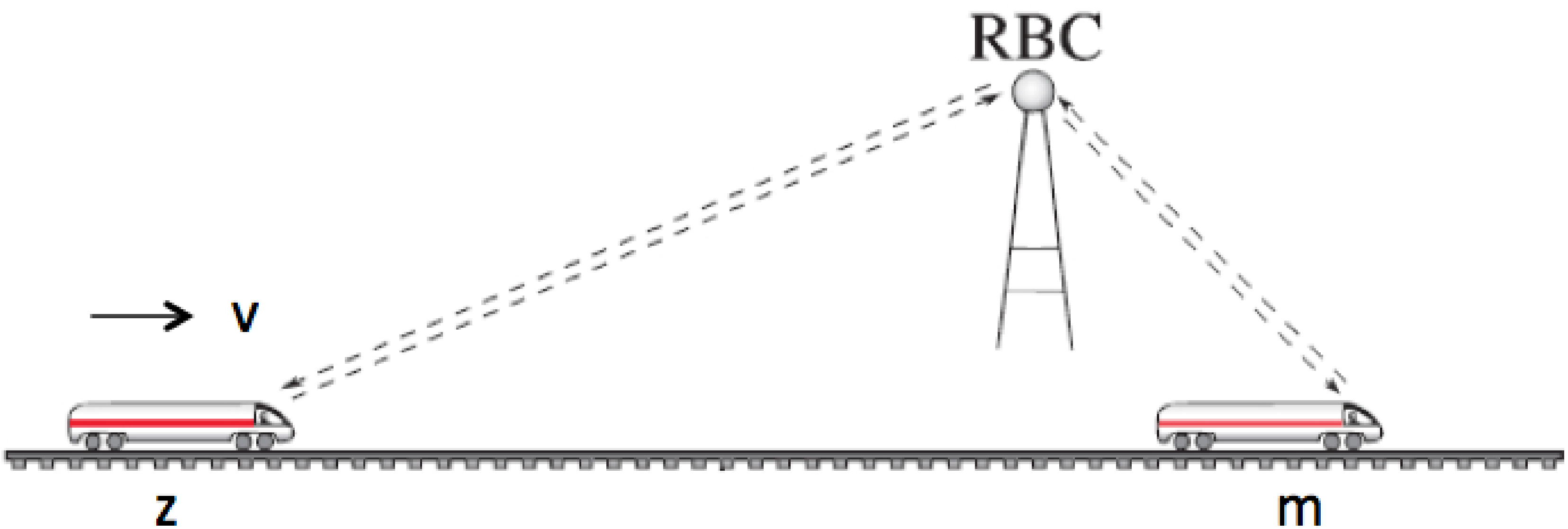


- Two trains are sent some information by Radio BroadCasting



- The second train is in position z

- Two trains are sent some information by Radio BroadCasting



- The second train is in position z

- It is made aware of a position m where it should at the latest stop

Train Control: Constraints and Goal

Train Control: Constraints and Goal

- The controller in the second train reacts every other ϵ seconds

Train Control: Constraints and Goal

- The controller in the second train reacts every other ϵ seconds

- It can change the acceleration of the train according to 3 values:

  Accelerations are: $\boldsymbol{A}$, $\boldsymbol{-b}$, or $\mathbf{0}$, where $\boldsymbol{A}$ and $\boldsymbol{b}$ are positive

Train Control: Constraints and Goal

- The controller in the second train reacts every other ϵ seconds

- It can change the acceleration of the train according to 3 values:

  Accelerations are: A, $-b$, or 0, where A and b are positive

- The speed should never be greater than sl (speed limit)

Train Control: Constraints and Goal

- The controller in the second train reacts every other ϵ seconds

- It can change the acceleration of the train according to 3 values:

  Accelerations are: A, $-b$, or 0, where A and b are positive

- The speed should never be greater than sl (speed limit)

- The train should never go backwards

Train Control: Constraints and Goal

- The controller in the second train reacts every other ϵ seconds

- It can change the acceleration of the train according to 3 values:

  Accelerations are: A, $-b$, or 0, where A and b are positive

- The speed should never be greater than sl (speed limit)

- The train should never go backwards

- Goal: Calculate the best acceleration at each controller's reaction.

- The second train is at position z and the "goal" is at position m

- The second train is at position z and the "goal" is at position m

- The train has a mass M and a speed v

- The second train is at position z and the "goal" is at position m

- The train has a mass M and a speed v

- In order to stop before m, the brake (deceleration b) should "absorb" the kinetic energy of the train ($\frac{Mv^2}{2}$):

- The second train is at position z and the "goal" is at position m

- The train has a mass M and a speed v

- In order to stop before m, the brake (deceleration b) should "absorb" the kinetic energy of the train ($\frac{Mv^2}{2}$):

$$Mb(m - z) \geq \frac{Mv^2}{2}$$

- The second train is at position z and the "goal" is at position m

- The train has a mass M and a speed v

- In order to stop before m, the brake (deceleration b) should "absorb" the kinetic energy of the train ($\frac{Mv^2}{2}$):

$$Mb(m - z) \geq \frac{Mv^2}{2}$$

that is

$$2b(m - z) \geq v^2$$

- The second train is at position z and the "goal" is at position m

- The train has a mass M and a speed v

- In order to stop before m, the brake (deceleration b) should "absorb" the kinetic energy of the train ($\frac{Mv^2}{2}$):

$$Mb(m - z) \geq \frac{Mv^2}{2}$$

that is

$$2b(m - z) \geq v^2$$

- This is the main invariant to be maintained

- At each control time (every other ϵ seconds), the invariant to be maintained is:

$$2b(m - z) \geq v^2$$

- At each control time (every other ϵ seconds), the invariant to be maintained is:

$$2b(m - z) \geq v^2$$

- If the speed is v and acceleration is a at position z,

- At each control time (every other ϵ seconds), the invariant to be maintained is:

$$2b(m - z) \geq v^2$$

- If the speed is v and acceleration is a at position z,
- after ϵ seconds, the speed will be $v + a\epsilon$

- At each control time (every other ϵ seconds), the invariant to be maintained is:

$$2b(m - z) \geq v^2$$

- If the speed is v and acceleration is a at position z,
- after ϵ seconds, the speed will be $v + a\epsilon$
- and the position will be $z + v\epsilon + a\frac{\epsilon^2}{2}$.

- At each control time (every other ϵ seconds), the invariant to be maintained is:

$$2b(m - z) \geq v^2$$

- If the speed is v and acceleration is a at position z,
- after ϵ seconds, the speed will be $v + a\epsilon$
- and the position will be $z + v\epsilon + a\frac{\epsilon^2}{2}$. We must then have:

$$2b(m - z - v\epsilon - a\frac{\epsilon^2}{2}) \geq (v + a\epsilon)^2$$

- At each control time (every other ϵ seconds), the invariant to be maintained is:

$$2b(m - z) \geq v^2$$

- If the speed is v and acceleration is a at position z,
- after ϵ seconds, the speed will be $v + a\epsilon$
- and the position will be $z + v\epsilon + a\frac{\epsilon^2}{2}$. We must then have:

$$2b(m - z - v\epsilon - a\frac{\epsilon^2}{2}) \geq (v + a\epsilon)^2$$

that is

$$2b(m - z) \geq v^2 + (a\epsilon^2 + 2v\epsilon)(a + b)$$

- We must have the following after ϵ seconds:

$$2b(m - z) \geq v^2 + (a\epsilon^2 + 2v\epsilon)(a + b)$$

- We must have the following after ϵ seconds:

$$2b(m - z) \geq v^2 + (a\epsilon^2 + 2v\epsilon)(a + b)$$

- The choice of the new acceleration can be A if

$$2b(m - z) \geq v^2 + (a\epsilon^2 + 2v\epsilon)(A + b)$$

- We must have the following after ϵ seconds:

$$2b(m - z) \geq v^2 + (a\epsilon^2 + 2v\epsilon)(a + b)$$

- The choice of the new acceleration can be A if

$$2b(m - z) \geq v^2 + (a\epsilon^2 + 2v\epsilon)(A + b)$$

- Otherwise, the acceleration should be -b (braking), resulting in:

$$2b(m - z) \geq v^2$$

- After the choice of acceleration, A or -b, the speed of the train is:

$$v + a\epsilon$$

- After the choice of acceleration, A or -b, the speed of the train is:

$$v + a\epsilon$$

- If $v + a\epsilon > sl$, we must choose a 0 acceleration (instead of A)

- After the choice of acceleration, A or -b, the speed of the train is:

$$v + a\epsilon$$

- If $v + a\epsilon > sl$, we must choose a 0 acceleration (instead of A)

- We have the additional invariant: $v \in 0 \,..\, sl$

- After the choice of acceleration, A or -b, the speed of the train is:

$$v + a\epsilon$$

- If $v + a\epsilon > sl$, we must choose a 0 acceleration (instead of A)

- We have the additional invariant: $v \in 0 \,..\, sl$

- We have thus three different controller decisions:
    - decision 1: acceleration -b
    - decision 2: acceleration A
    - decision 3: acceleration 0

- If the speed and position are v and z, then after ϵ seconds:

- If the speed and position are v and z, then after ϵ seconds:

- the new speed of the train will be:

    - drive 1: if $v + a\epsilon \geq 0$ then $v + a\epsilon$

    - drive 2: if $v + a\epsilon < 0$ then 0

- If the speed and position are v and z, then after ϵ seconds:

- the new speed of the train will be:

  - drive 1: if $v + a\epsilon \geq 0$ then $v + a\epsilon$

  - drive 2: if $v + a\epsilon < 0$ then 0

- the new position of the train will be:

  - drive 1: if $v + a\epsilon \geq 0$ then $z + v\epsilon + a\frac{\epsilon^2}{2}$

  - drive 2: if $v + a\epsilon < 0$ then $z + \frac{v^2}{2b}$ (the train stops after time $\frac{v}{b}$)

- We presented an approach to develop hybrid systems in Event-B

- We presented an approach to develop hybrid systems in Event-B

- This approach did not require adding new features to Event-B

Conclusion and Future Work

- We presented an approach to develop hybrid systems in Event-B

- This approach did not require adding new features to Event-B

- The only thing that will be necessary in Event-B are Real Numbers

Conclusion and Future Work

- We presented an approach to develop hybrid systems in Event-B

- This approach did not require adding new features to Event-B

- The only thing that will be necessary in Event-B are Real Numbers

- This will be done through the very important Theory plug-in (Issam Maamria, Michael Butler)

Conclusion and Future Work

- We presented an approach to develop hybrid systems in Event-B

- This approach did not require adding new features to Event-B

- The only thing that will be necessary in Event-B are Real Numbers

- This will be done through the very important Theory plug-in (Issam Maamria, Michael Butler)

- Continuous variables are not defined by differential equations

Thank you for listening