Barrier Certificate Generation for Safety Verification of Hybrid System for a Given Period of Time

Ting Gan   Liyun Dai   Bican Xia
gant@pku.edu.cn
LMAM & School of Mathematical Sciences, Peking University

MACIS2013

Dec 13, 2013

Outline:

The problem

Some sufficient conditions

Solving with SOSTOOLS/MATLAB

An example

1. The problem

A continuous system is defined as an ordinary differential equation(ODE)

$$\dot{x} = f(x)$$

Where $x \in \mathbb{R}^n$ and f is a Lipschitz continuous vector function form $\mathbb{R}^n$ to $\mathbb{R}^n$

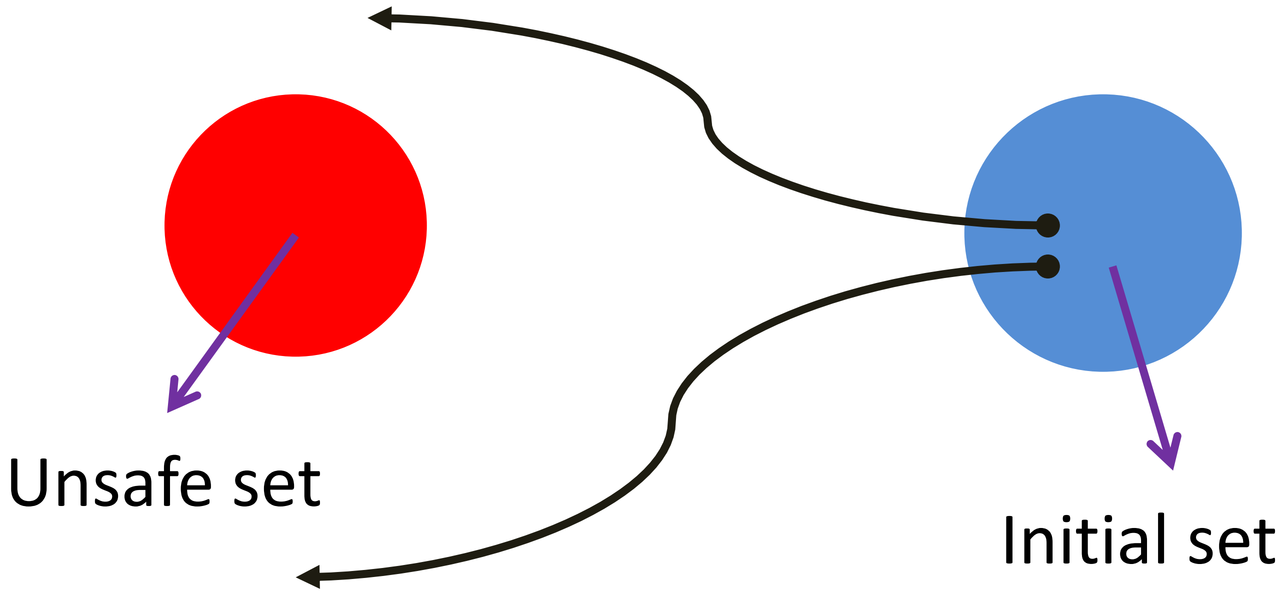
Given a continuous system $\dot{x} = f(x)$,

an initial set $\mathbf{I}$ and an unsafe set $\mathbf{U}$.

Given a continuous system $\dot{x} = f(x)$,

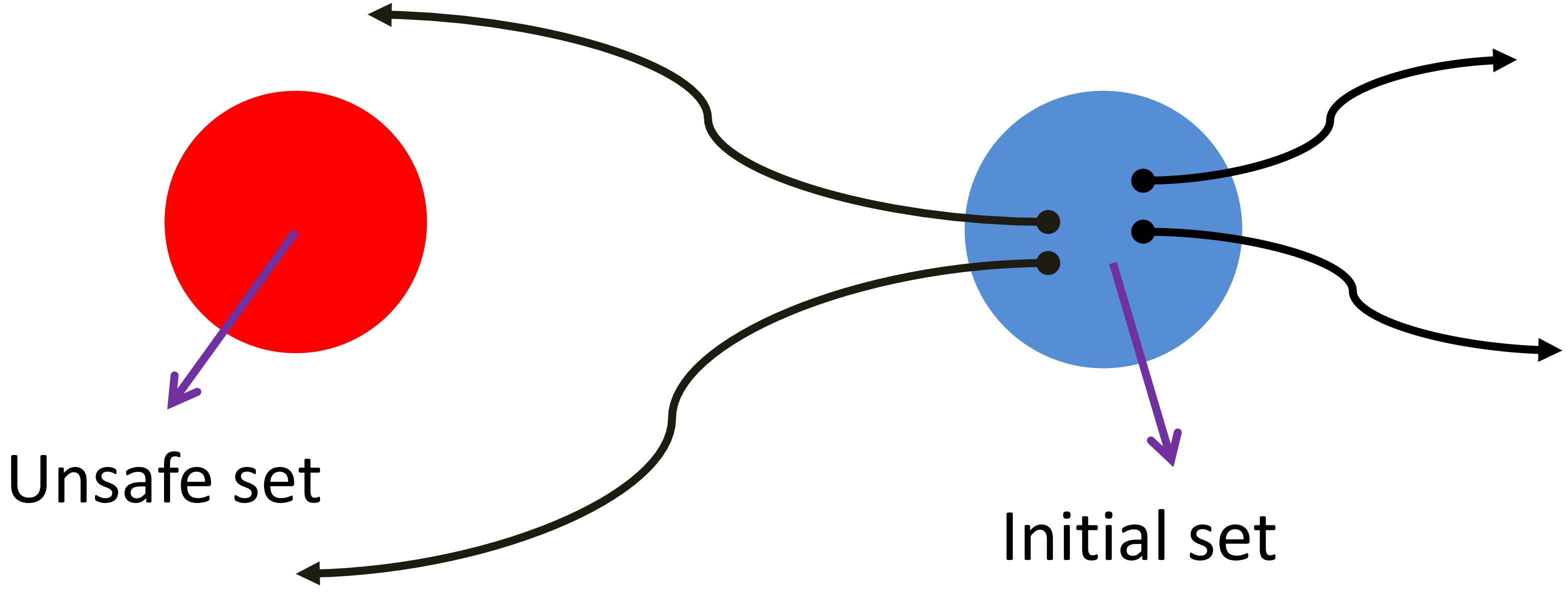
an initial set I and an unsafe set $\mathbf{U}$.

Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set U .

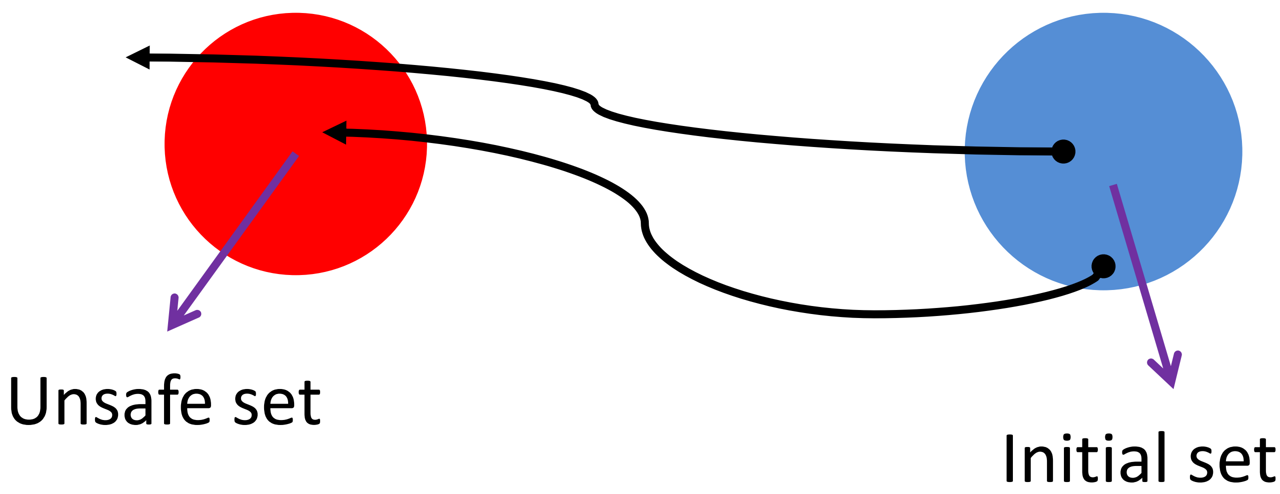


Given a continuous system $\dot{x} = f(x)$,

an initial set I and an unsafe set $\mathbf{U}$.



Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set $\mathbf{U}$.

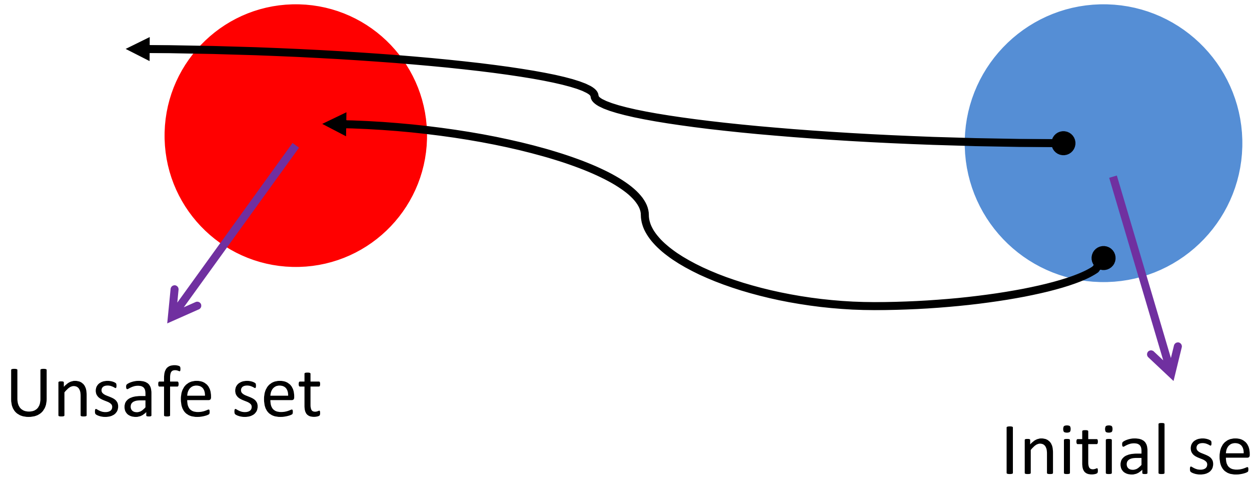


Our problem:

How to verify the safety of the continuous system in a bounded time ,such as $t \leq 1$?

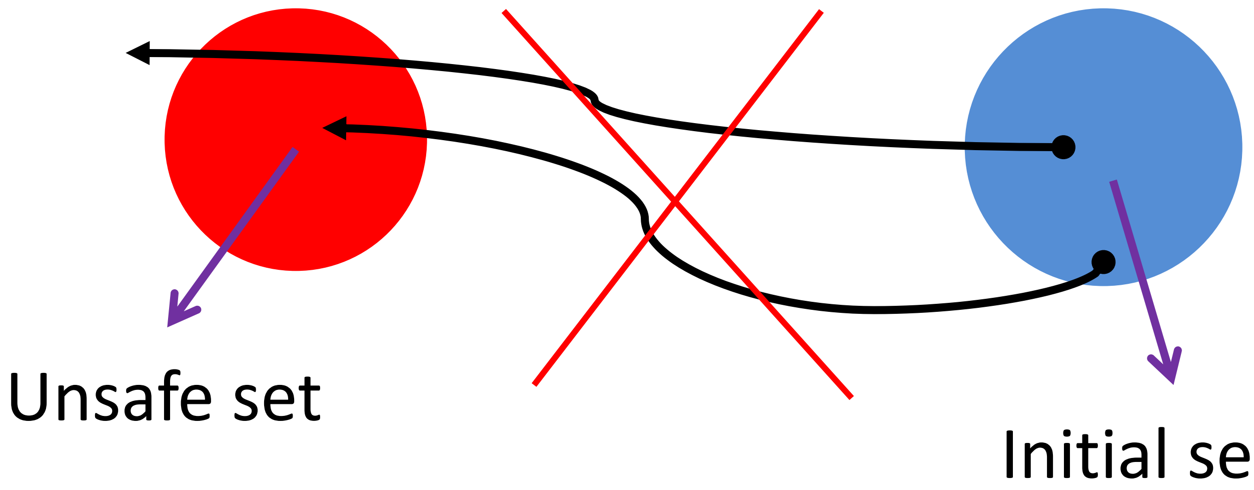
Our problem:

How to verify the safety of the continuous system in a bounded time ,such as $t \leq 1$?



Our problem:

How to verify the safety of the continuous system in a bounded time ,such as $t \leq 1$?



2. Some sufficient conditions

Lemma 1. Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set U , for any given $\lambda < 0$, $\eta > 0$, if there exists a real-valued function $\varphi(x) \in C^1$ satisfying the following formulae:

Lemma 1. Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set U , for any given $\lambda < 0$, $\eta > 0$, if there exists a real-valued function $\varphi(x) \in \mathrm{C}^1$ satisfying the following formulae:

$$condition\ 1: \quad \forall\, x \in I:\ \varphi(x) \leq 0$$

Lemma 1. Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set U , for any given $\lambda < 0$, $\eta > 0$, if there exists a real-valued function $\varphi(x) \in C^1$ satisfying the following formulae:

$$condition\ 1: \quad \forall\, x \in I: \ \varphi(x) \leq 0$$

$$condition\ 2: \quad \forall x \in \mathbb{R}^n: \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \eta \leq 0$$

Note: $\mathcal{L}_f\varphi(x) = \frac{d\varphi}{dx} f$,is the **lie derivative**

Lemma 1. Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set U , for any given $\lambda < 0$, $\eta > 0$, if there exists a real-valued function $\varphi(x) \in C^1$ satisfying the following formulae:

$$\boxed{condition\ 1: \quad \forall\, x \in I:\ \varphi(x) \le 0}$$

$$\boxed{condition\ 2: \quad \forall x \in \mathbb{R}^n\!:\ \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \eta \le 0}$$

$$\boxed{condition\ 3: \quad \forall\, x \in U:\ \varphi(x) \ge \eta}$$

Lemma 1. Given a continuous system $\dot{x} = f(x)$, an initial set I and an unsafe set U , for any given $\lambda < 0$, $\eta > 0$, if there exists a real-valued function $\varphi(x) \in C^1$ satisfying the following formulae:

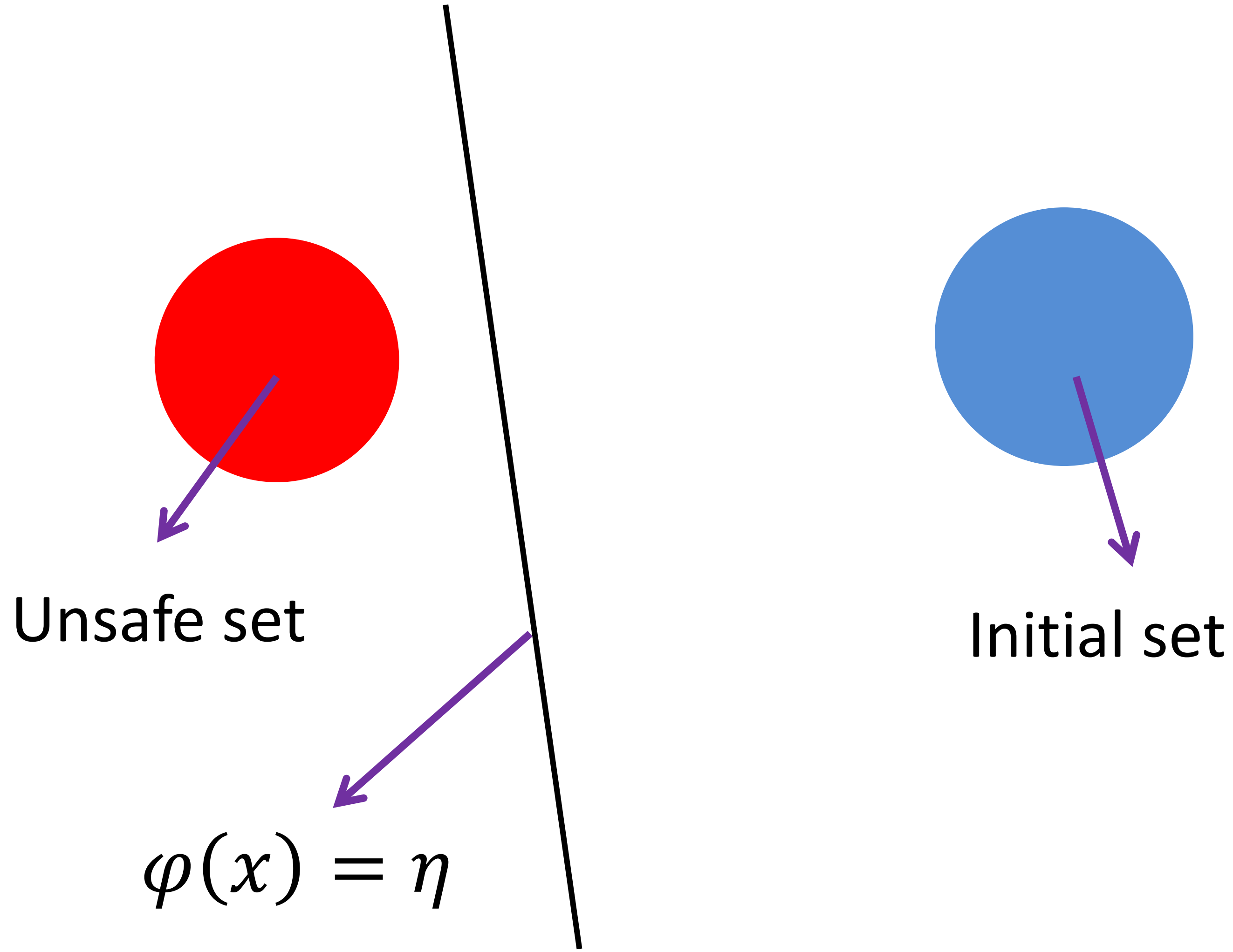
$$condition\ 1: \quad \forall\, x \in I: \ \varphi(x) \leq 0$$

$$condition\ 2: \quad \forall x \in \mathbb{R}^n\!: \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \eta \leq 0$$

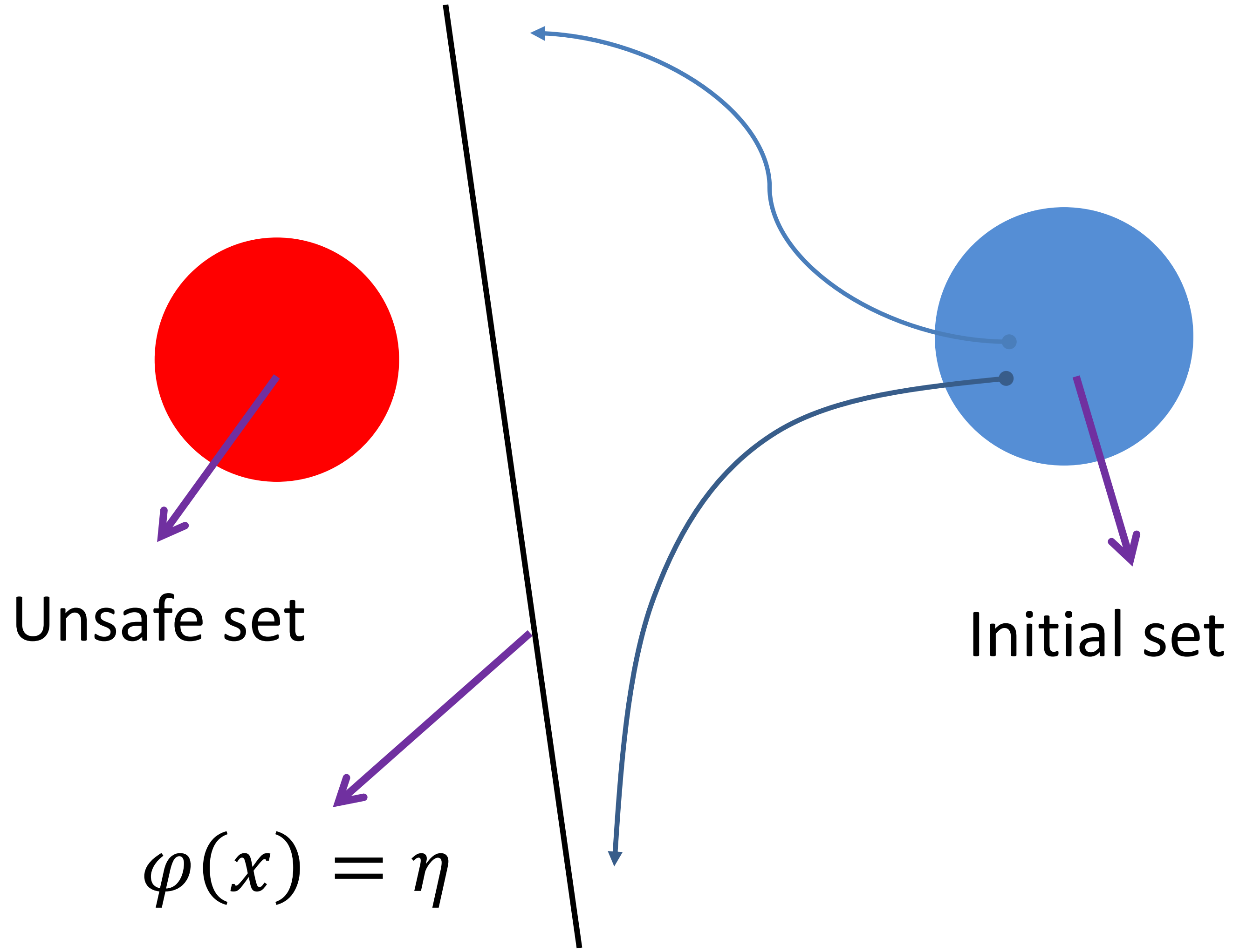
$$condition\ 3: \quad \forall\, x \in U: \ \varphi(x) \geq \eta$$

Then, the safety property is satisfied when $t \in [0,1]$.

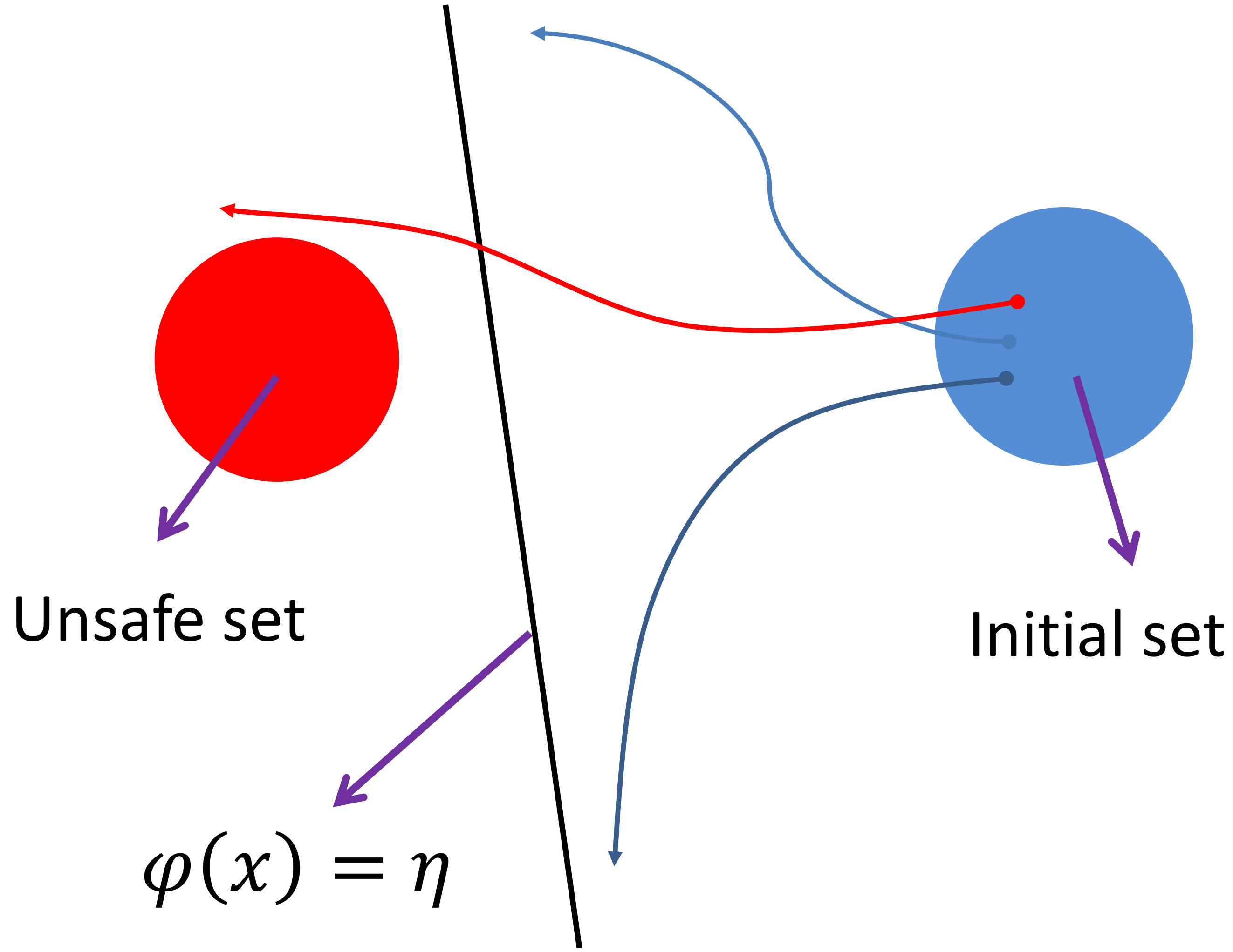
A diagram briefly show the Lemma 1.



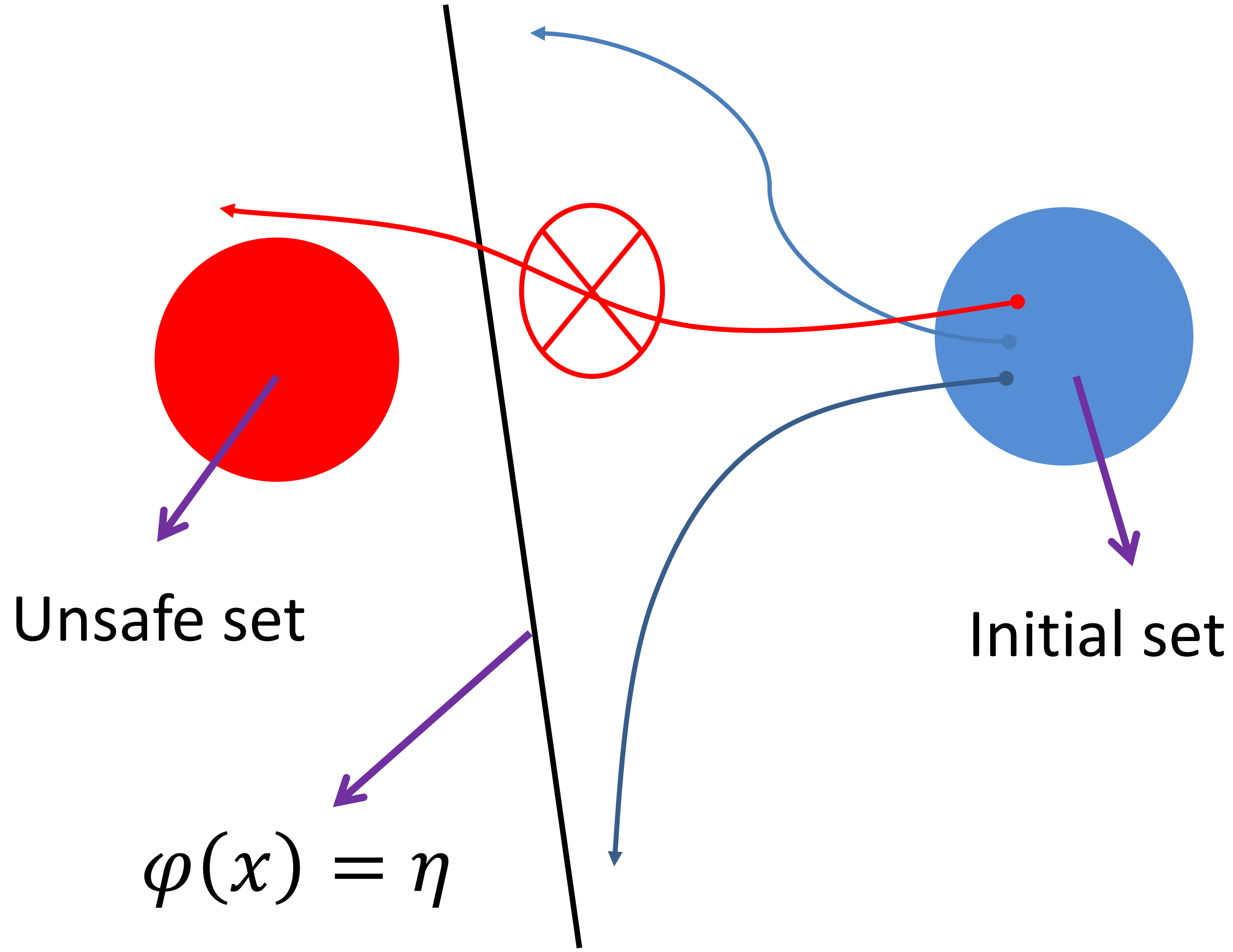
A diagram briefly show the Lemma 1.



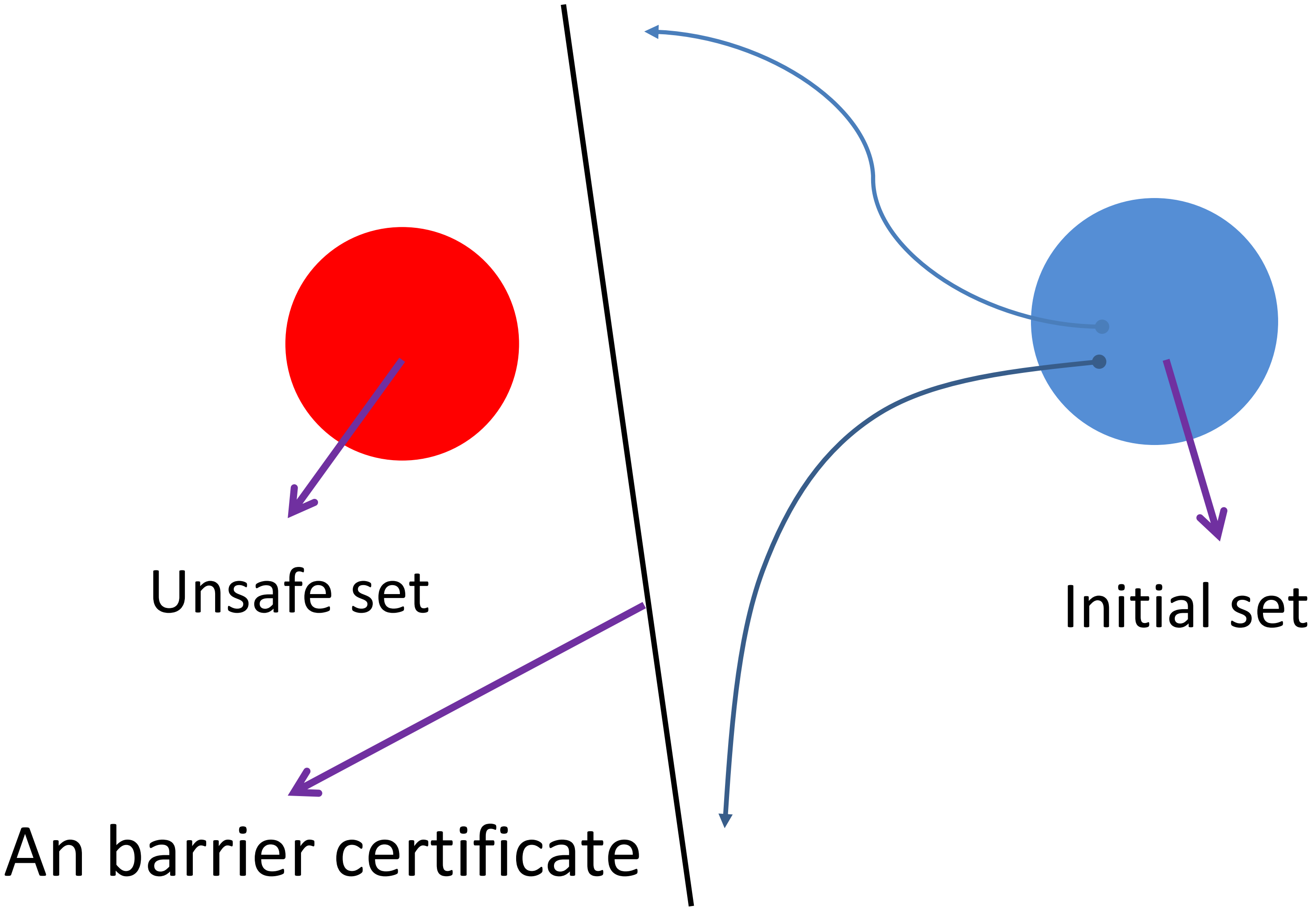
A diagram briefly show the Lemma 1.



A diagram briefly show the Lemma 1.



A diagram briefly show the Lemma 1.



Theorem 1. $I, U, \lambda, \eta, \varphi$ are defined the same with Lemma 1. Only condition 2 is replaced by condition 4.

$$condition\ 1: \quad \forall\, x \in I: \ \varphi(x) \leq 0$$

$$condition\ 4: \quad \forall x \in \mathbb{R}^n: \mathcal{L}_f \varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} \leq 0$$

$$condition\ 3: \quad \forall\, x \in U: \ \varphi(x) \geq \eta$$

Then the safety property is satisfied when $t \in [0, T]$.

Theorem 1. $I, U, \lambda, \eta, \varphi$ are defined the same with Lemma 1. Only condition 2 is replaced by condition 4.

$$condition\ 1: \quad \forall\, x \in I: \ \varphi(x) \leq 0$$

$$condition\ 4: \quad \forall x \in \mathbb{R}^n: \mathcal{L}_f \varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} \leq 0$$

$$condition\ 3: \quad \forall\, x \in U: \ \varphi(x) \geq \eta$$

Then the safety property is satisfied when $t \in [0, T]$.

Proof: Let $\xi = \frac{t}{T}$, replace t by ξ. From lemma 1, it is easy to see Theorem 1 hold.

Theorem 2. $I, U, \lambda, \eta, \varphi$ are defined the same with Theorem 1. Only condition 4 is replaced by condition 5. Where B is an over-approximation set of the reachable set without time limited.

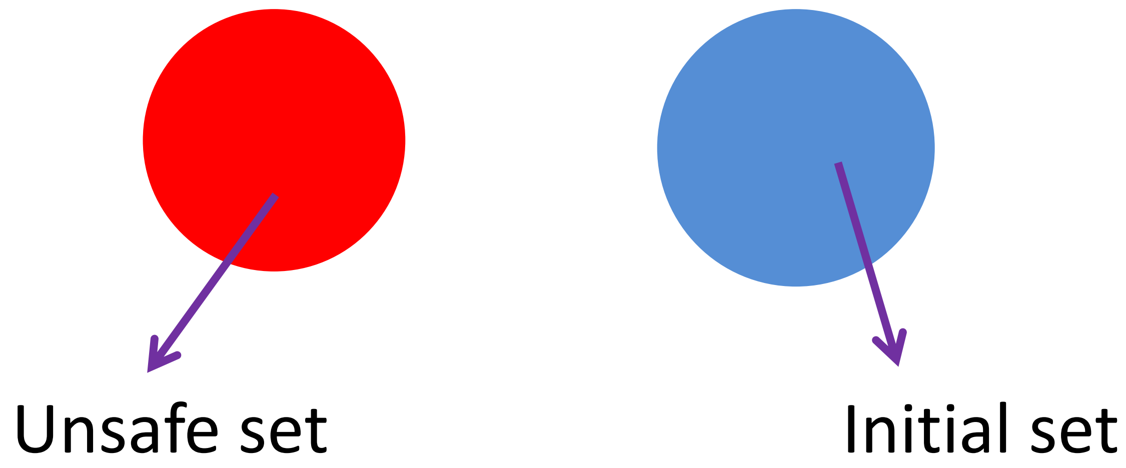
$$condition\ 1: \quad \forall\, x \in I: \ \varphi(x) \leq 0$$

$$condition\ 5: \quad \forall x \in B: \ \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} \leq 0$$

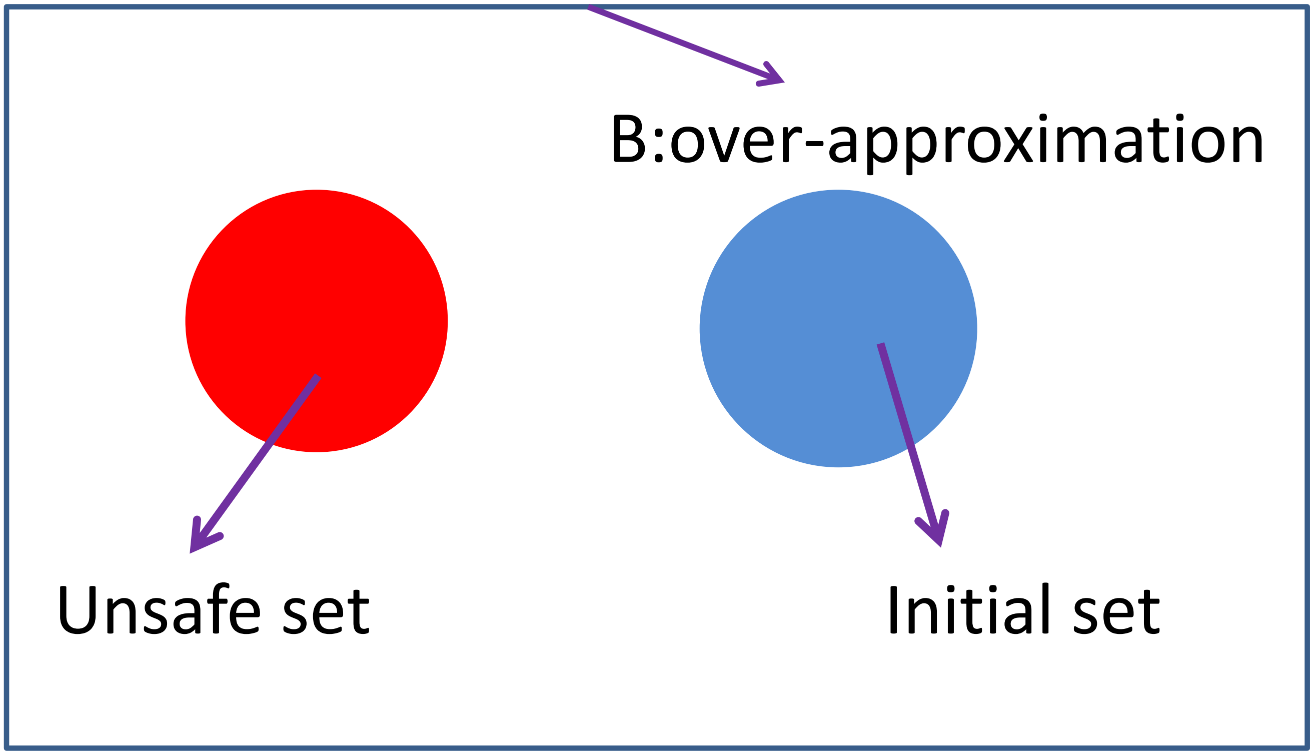
$$condition\ 3: \quad \forall\, x \in U: \ \varphi(x) \geq \eta$$

Then the safety property is satisfied when $t \in [0, T]$.

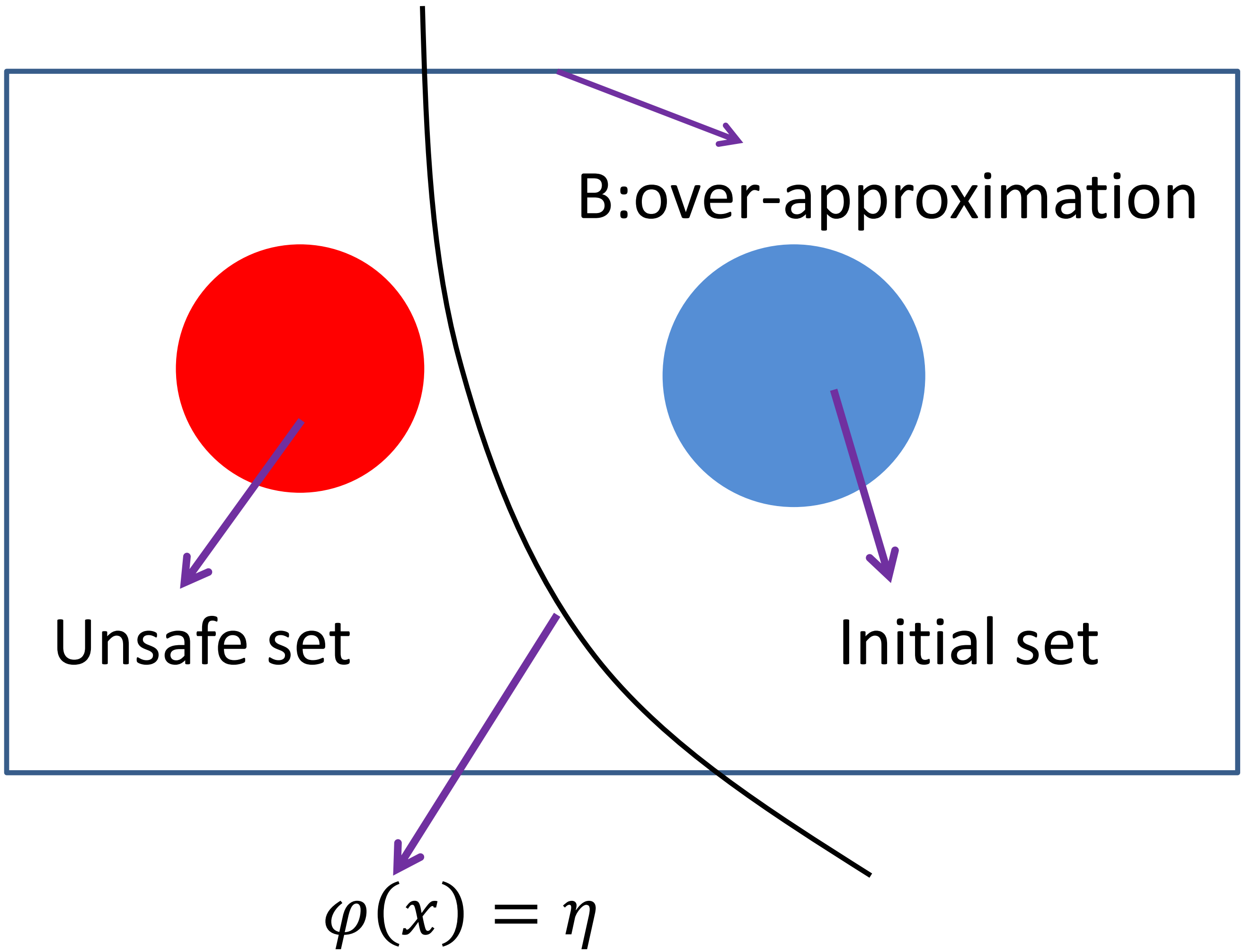
A diagram briefly show the Theorem 2.



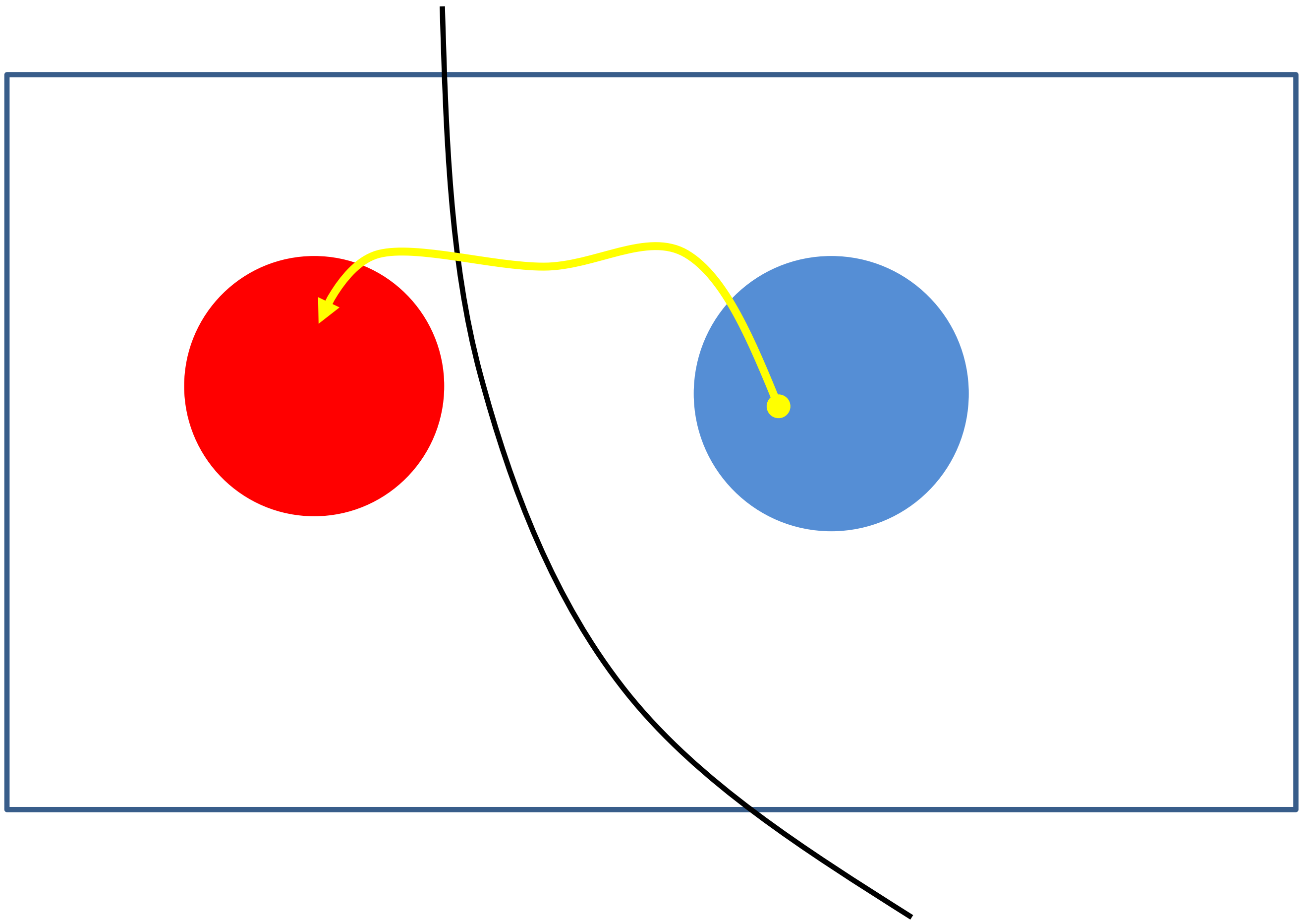
A diagram briefly show the Theorem 2.



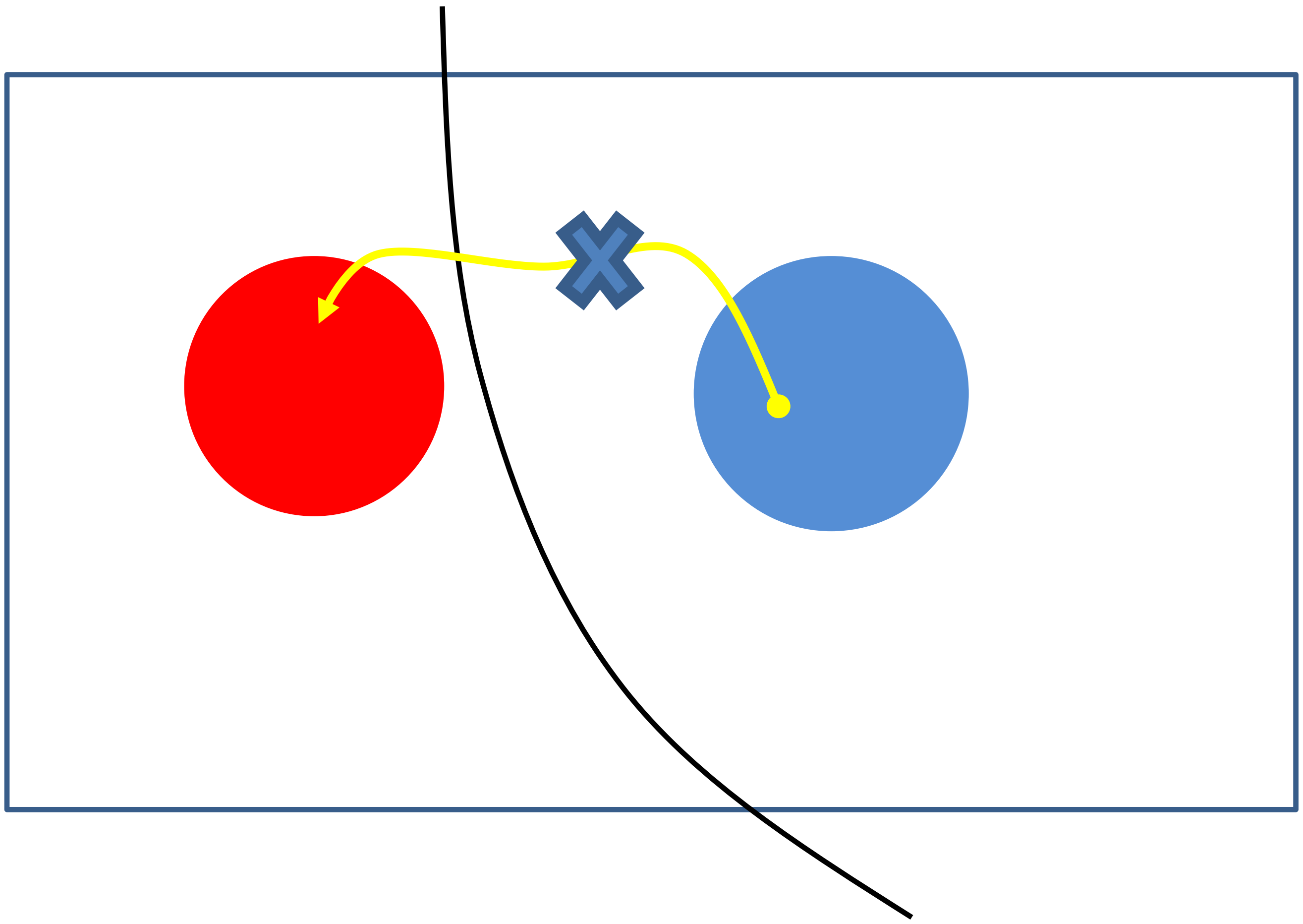
A diagram briefly show the Theorem 2.



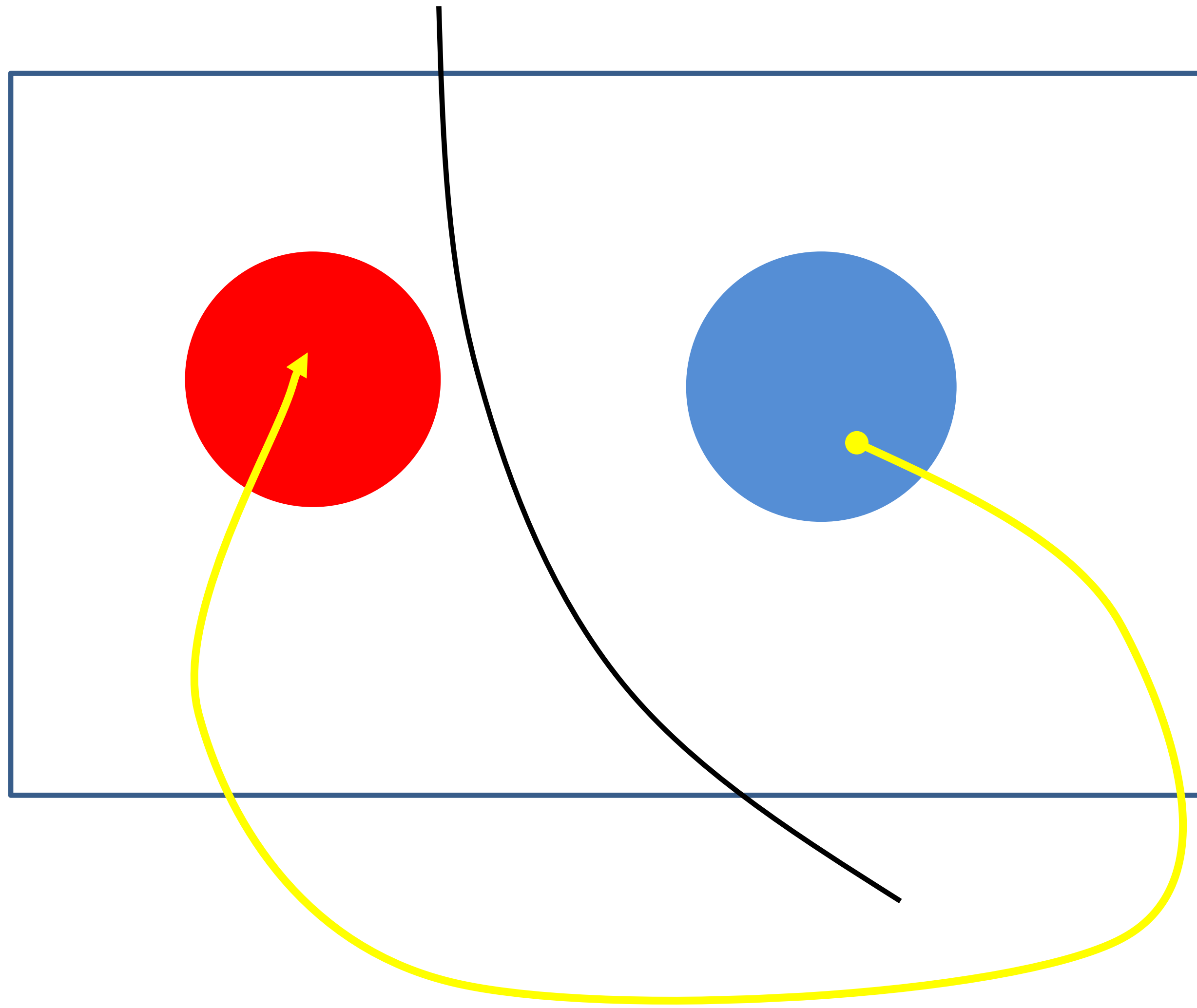
A diagram briefly show the Theorem 2.



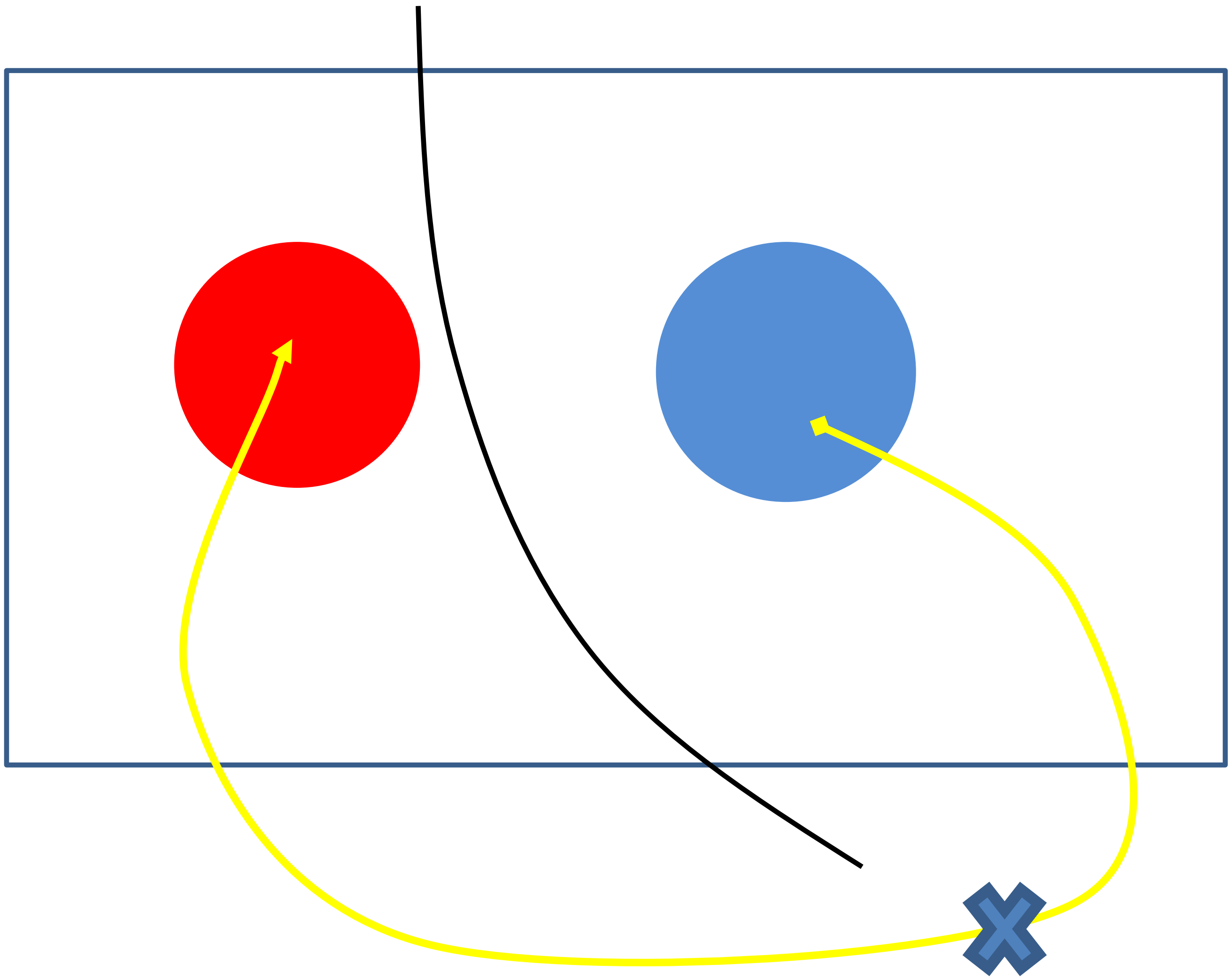
A diagram briefly show the Theorem 2.



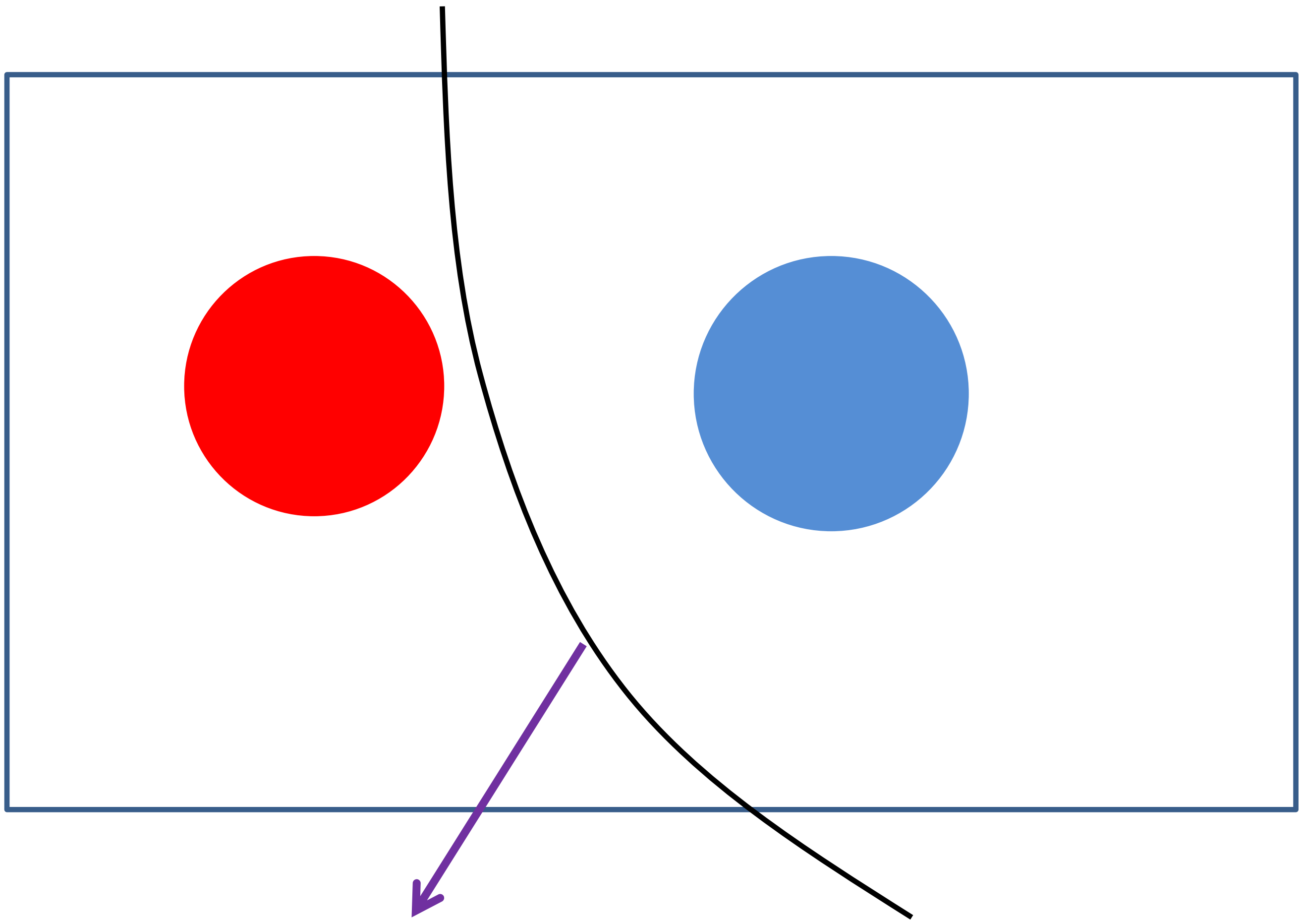
A diagram briefly show the Theorem 2.



A diagram briefly show the Theorem 2.



A diagram briefly show the Theorem 2.



Theorem 1 and Theorem 2 give some sufficient conditions to guard a continuous system to be safe.

$$(C1)\begin{cases} \forall\, x \in I:\ \varphi(x) \le 0 \\ \forall x \in \mathbb{R}^n\colon \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} \le 0 \\ \forall\, x \in U:\ \varphi(x) \ge \eta \end{cases}$$

$$(C2)\begin{cases} \forall\, x \in I:\ \varphi(x) \le 0 \\ \forall x \in B\colon \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} \le 0 \\ \forall\, x \in U:\ \varphi(x) \ge \eta \end{cases}$$

Next we need to find a φ satisfy (C1) or (C2)

Actually, we also have a sufficient condition to guard $B \geq 0$ is a over-approximation of the reachable set of the continuous system.

$$(C3)\begin{cases} \forall\, x \in I : B(x) \geq 0 \\ \forall x \in \mathbb{R}^n \colon \mathcal{L}_f B(x) - \gamma B(x) \geq 0 \end{cases}$$

For any given $\gamma \in \mathbb{R}$, if (C3) is satisfy for B, then $B \geq 0$ is an over-approximation of the reachable set of the continuous system. We confusingly using B to be the set $\{x | B(x) \geq 0\}$.

3. Solving with SOSTOOLS/MATLAB

The basic feasibility problem in SOS programming will be formulated as follow:

Find

$$polynomials\ p_i(x), \qquad for\ i = 1,2, \dots, N_1$$

$$sums\ of\ squares\ p_i(x), \qquad for\ \ i = N_1 + 1, \dots, N$$

The basic feasibility problem in SOS programming will be formulated as follow:

Find

$$polynomials\ p_i(x), \qquad for\ i = 1,2,\dots,N_1$$

$$sums\ of\ squares\ p_i(x), \qquad for\ \ i = N_1 + 1,\dots,N$$

Such that

$$a_{0,j}(x) + p_1(x)a_{1,j}(x) + \cdots + p_N a_{N,j} = 0, \qquad for\ j = 1,2,\dots,j_1$$

The basic feasibility problem in SOS programming will be formulated as follow:

Find

$$polynomials\ p_i(x), \qquad for\ i = 1,2,\dots,N_1$$

$$sums\ of\ squares\ p_i(x), \qquad for\ \ i = N_1 + 1,\dots,N$$

Such that

$$a_{0,j}(x) + p_1(x)a_{1,j}(x) + \cdots + p_N a_{N,j} = 0, \qquad for\ j = 1,2,\dots,j_1$$

$$a_{0,j}(x) + p_1(x)a_{1,j}(x) + \cdots + p_N a_{N,j} \qquad are\ sums\ of\ squares,$$
$$for\ j = j_1 + 1,\dots,j$$

Convert (C1) and (C2) to SOS feasibility problems.

We need to do SOS relaxation on (C1) and (C2).

And here we are just interest on the case that

$f(x)$ is a polynomial vector,

and initial set $\{x|I(x) \geq 0\}$,

unsafe set $\{x|U(x) \geq 0\}$,

where I, U are both polynomials.

$$
\text{(C1)} \begin{cases} \forall\, x \in I : \ \varphi(x) \leq 0 \\ \forall x \in \mathbb{R}^n : \ \mathcal{L}_f \varphi(x) - \ \lambda\varphi(x) - \frac{\eta}{T} \leq 0 \\ \forall\, x \in U : \ \ \varphi(x) \geq \eta \end{cases}
$$

Find: polynomial φ , SOS polynomials u_1, u_2

Such that

$$
-\varphi(x) - u_1 I
$$

$$
-\mathcal{L}_f \varphi(x) + \lambda\varphi(x) + \frac{\eta}{T}
$$

$$
\varphi(x) - u_2 - \eta
$$

are all sums of square.

$$(\text{C2})\begin{cases} \forall\, x \in I :\ \varphi(x) \le 0 \\ \forall x \in B\!:\ \mathcal{L}_f\varphi(x) - \lambda\varphi(x) - \frac{\eta}{T} \le 0 \\ \forall\, x \in U :\ \varphi(x) \ge \eta \end{cases}$$

Find: polynomial φ , SOS polynomials u_1, u_2, u_3

Such that

$$-\varphi(x) - u_1 I$$

$$-\mathcal{L}_f\varphi(x) + \lambda\varphi(x) + \frac{\eta}{T} - u_2 B$$

$$\varphi(x) - u_3 - \eta$$

are all sums of square.

Before solving (C2), we can first solving (C3) to get an over-approximation set B.

$$\text{(C3)} \begin{cases} \forall\, x \in I : B(x) \geq 0 \\ \forall x \in \mathbb{R}^n : \mathcal{L}_f B(x) - \gamma B(x) \geq 0 \end{cases}$$

Find: polynomial B , SOS polynomials u_1

Such that

$$B(x) - u_1 I$$

$$\mathcal{L}_f B(x) - \gamma B(x)$$

are both sums of square.

4. An example

Consider a continuous system:

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + \dfrac{1}{3}x^3 - y \end{cases}$$

Consider a continuous system:

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + \dfrac{1}{3}x^3 - y \end{cases}$$

Initial set $\{(x, y) | (x - 1.5)^2 + y^2 \leq 0.25\}$

Consider a continuous system:

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + \dfrac{1}{3}x^3 - y \end{cases}$$

Initial set $\{(x, y) | (x - 1.5)^2 + y^2 \leq 0.25\}$

Unsafe set $\{(x, y) | x^2 + y^2 \leq 0.16\}$

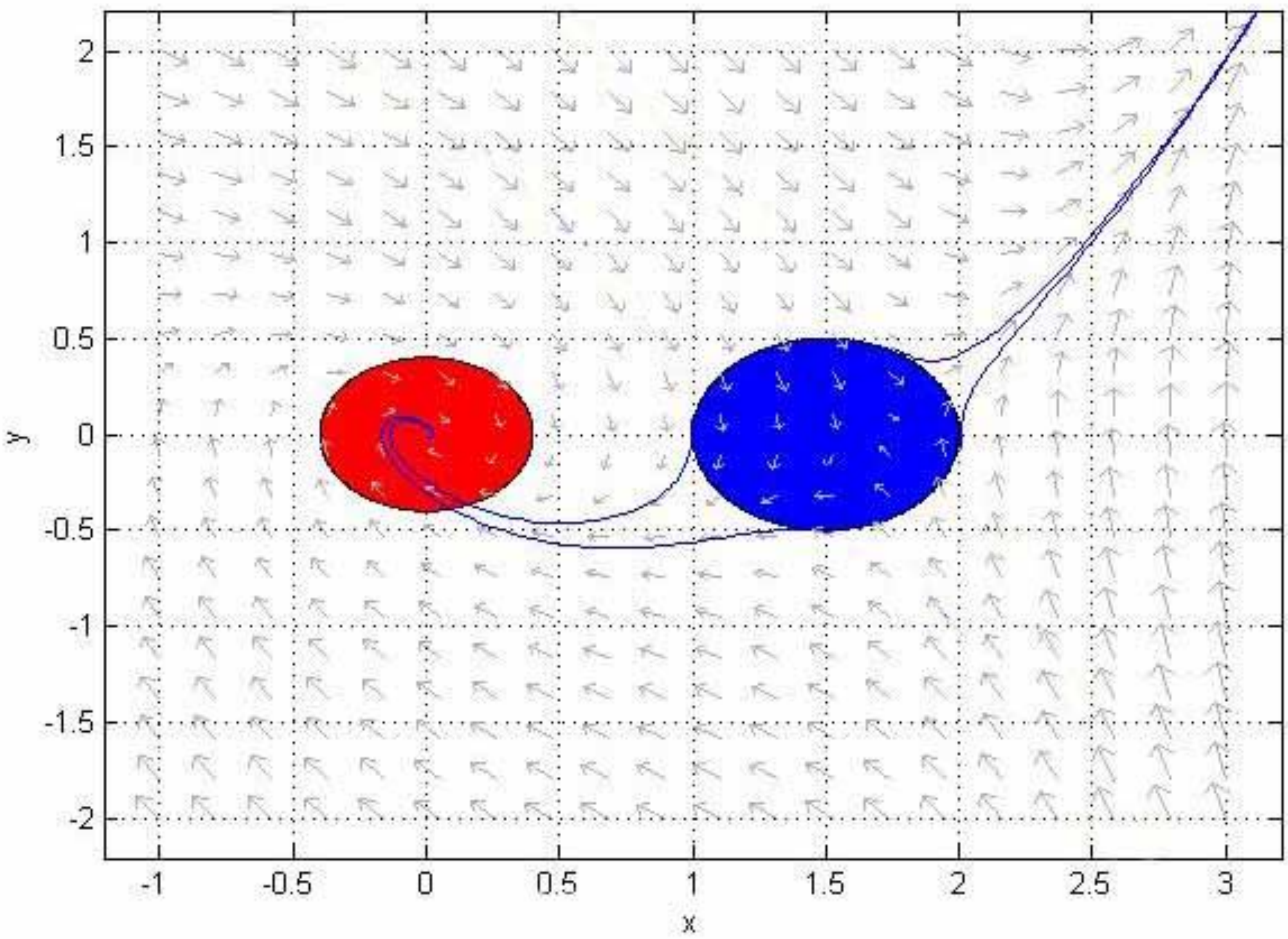
Consider a continuous system:

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + \dfrac{1}{3}x^3 - y \end{cases}$$

Initial set $\{(x, y) | (x - 1.5)^2 + y^2 \leq 0.25\}$

Unsafe set $\{(x, y) | x^2 + y^2 \leq 0.16\}$

We want to verify safety when $t \in [0,0.5]$



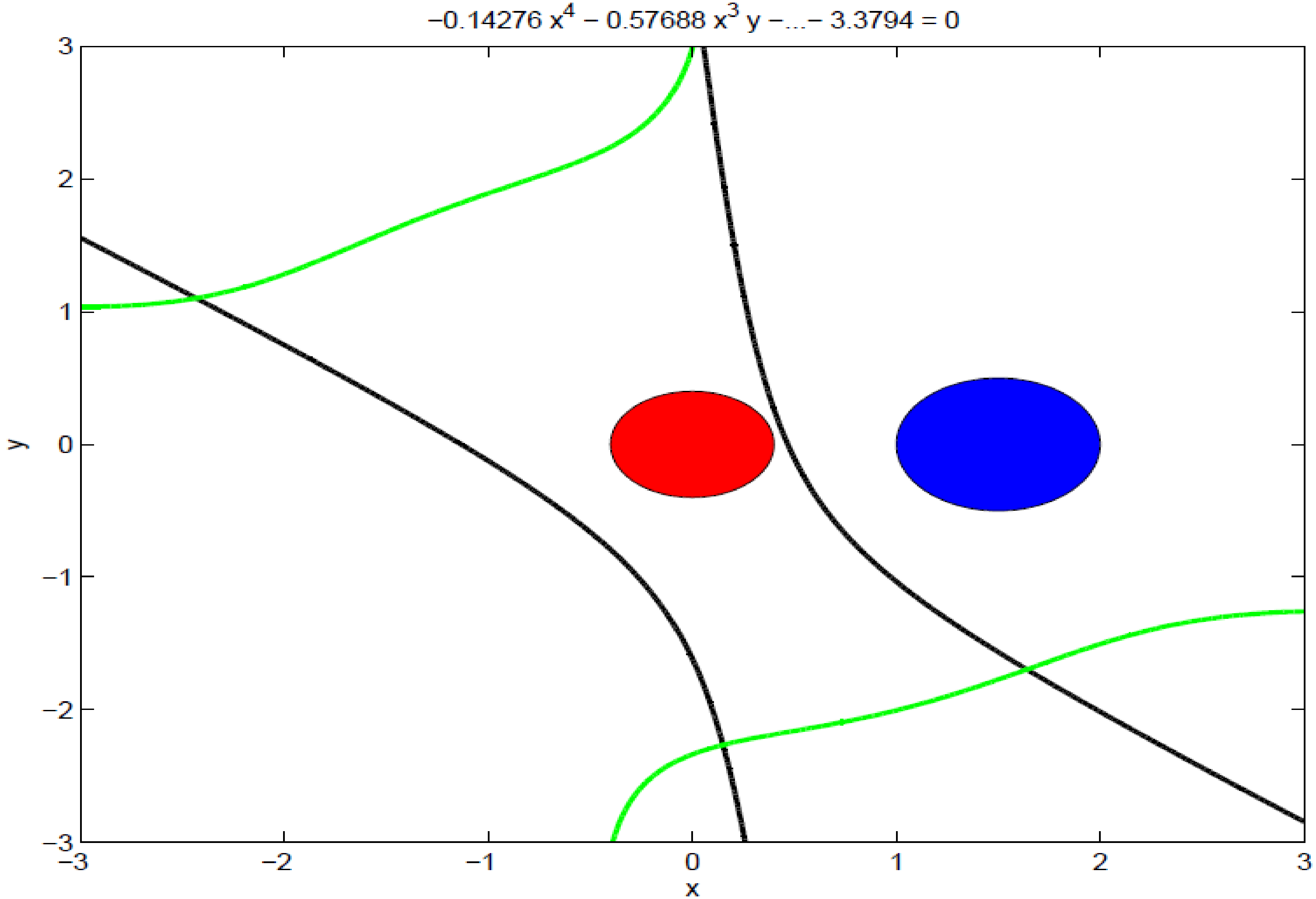
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
y
-1
-0.5
0
0.5
1
1.5
2
2.5
3
x

$$\gamma = -0.2$$

$$B = 0.14276x^4 + 0.57689x^3y + 0.073723x^3$$
$$+ 0.26373x\text{^}2y\text{^}2 + 0.20356x^2y + 0.052172x^2$$
$$+ 0.32187xy^3 + 0.12361xy^2 \text{- } 0.481xy$$
$$+ 0.37462x + 3.1289e\text{-}08y^4 + 0.05861y^3$$
$$\text{- } 0.52215\,y^2 \text{- } 0.092692y + 3.3794$$

$$\lambda = -0.4, \qquad \eta = 0.2,$$

$$\varphi = -0.23421x^2 - 0.32146xy - 0.15575x - 0.021073y^2 + 0.042566y + 0.32399$$


−0.14276 x4 − 0.57688 x3 y −...− 3.3794 = 0
y
x
3
2
1
0
−1
−2
−3
−3
−2
−1
0
1
2
3

THANK YOU

c^1: $first\ order\ continous\ differentiable$

reachable set:

$$Re = \{x(t) | t \geq 0, x(0) \in I, \dot{x} = f(x)\}$$

B is an over-approximation of Re :

$$Re \subset B$$

SOSTOOLS is a free, third-party MATLAB toolbox for solving sum of squares programs. The techniques behind it are based on the sum of squares decomposition for multivariate polynomials, which can be efficiently computed using semi-definite programming.