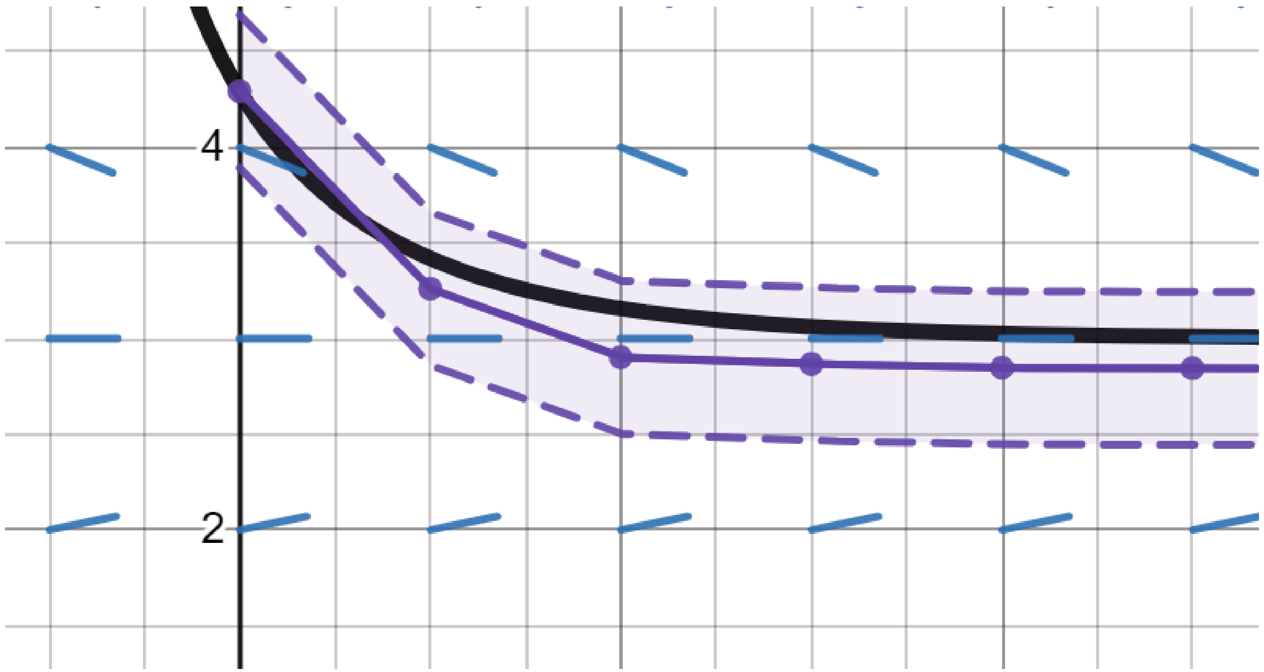
Numerical Extension ODE in KeYmaera X

Evelyn Kuo



Differential equations are fundamental to hybrid systems

$$
\begin{cases} \frac{d}{dt}x(t) = f(t, x(t)) \\ x(t_0) = x_0 \end{cases}
$$

- Differential equations model the physical world
- Initial value problem
- Analysis of differential equations
  - Mathematics: ODE theory (existence, uniqueness), numerical methods
  - Theorem provers: KeYmaera X

Pros/Cons of KeYmaera X ODE Tactics

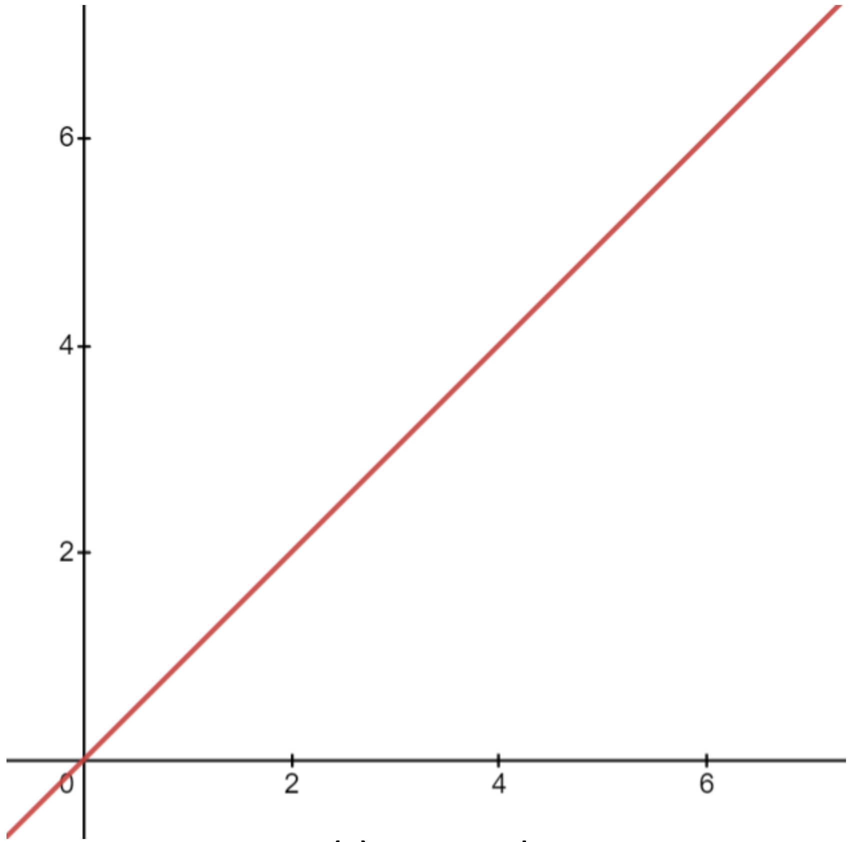
Actual Solution

- Easy to prove things knowing exact solution

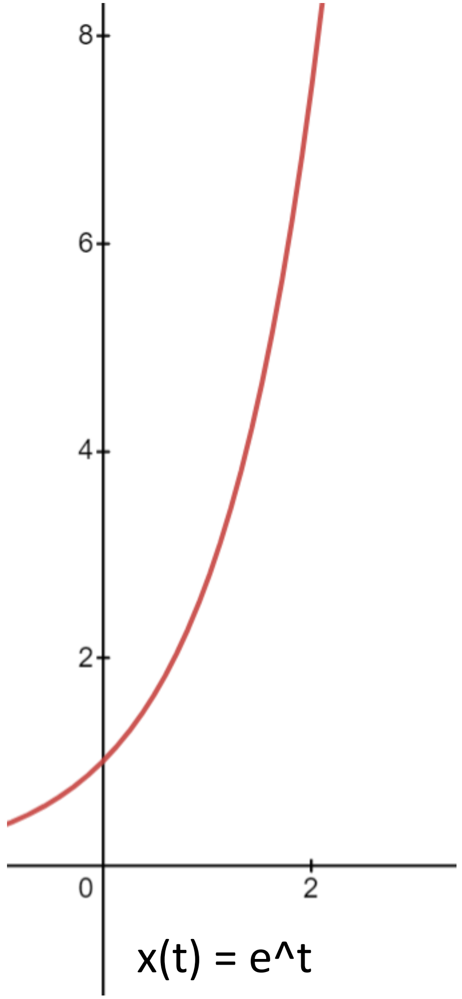
  {x’ = a}

- Not always easy to find or even represent solutions

  {x’ = x}



x(t) = 0 + a*t



x(t) = e^t

Pros/Cons of KeYmaera X ODE Tactics

Actual Solution

- Easy to prove things knowing exact solution

  $\{x' = a\}$

- Not always easy to find or even represent solutions

  $\{x' = x\}$

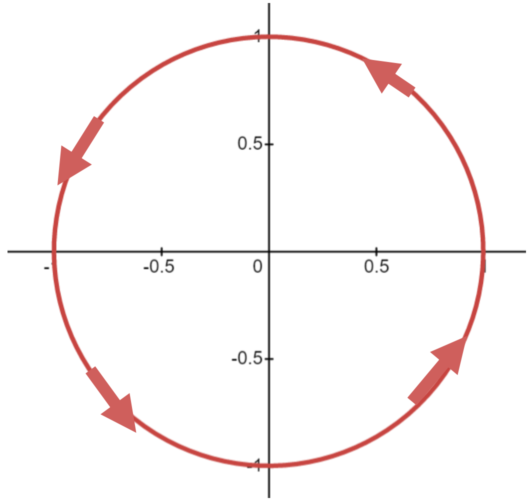
Differential Invariant

- Analyze trends in how quantities change without knowing exact solution

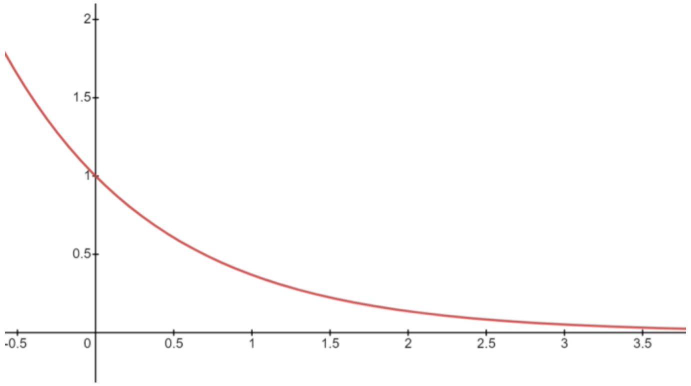
$[\{x'=-y, y'=x\}]\ x^2+y^2 = 1$

- Trends may not help in proof

$[\{x'=-x\}]x > 0$

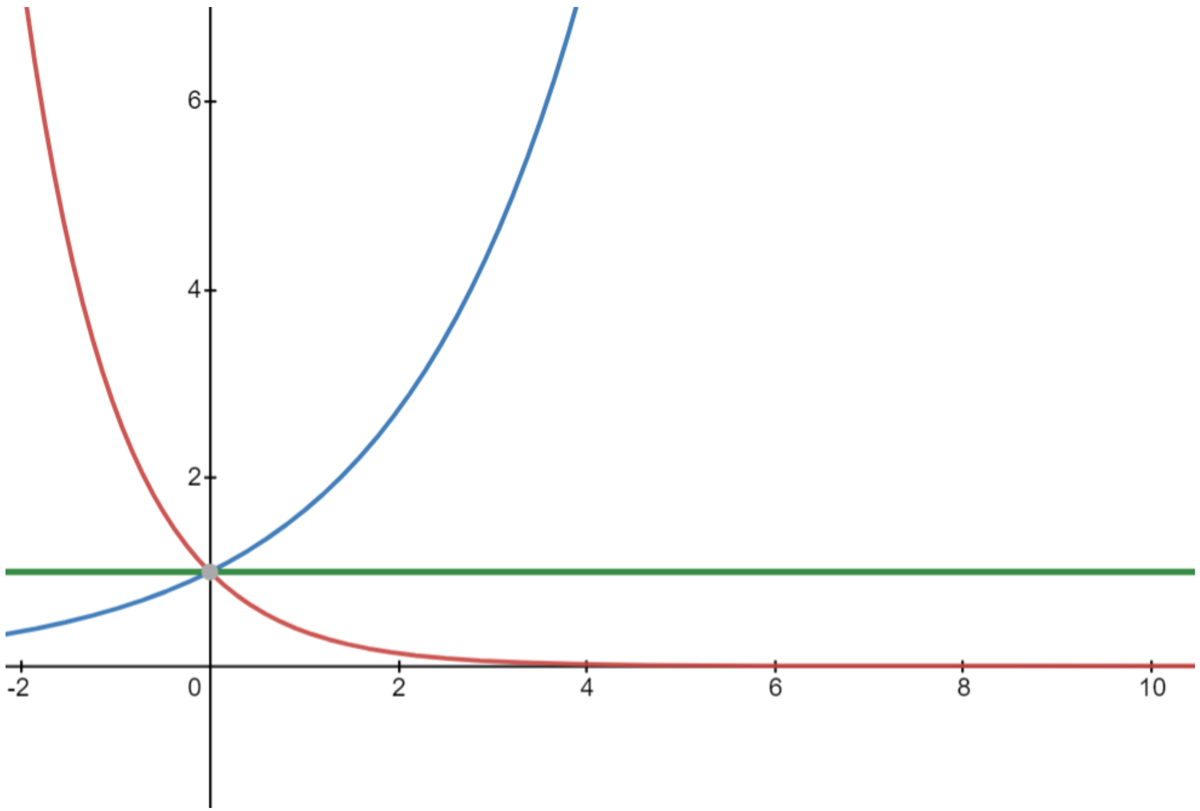


x(t) = cos(t)
y(t) = sin(t)



x(t) = e^{-t}

Pros/Cons of KeYmaera X ODE Tactics



x(t) = e^{-t}   y(t) = e^{t/2}   x(t)*y(t)^2 = 1

Differential Ghost

- Use ghost variable to analyze how quantities change without knowing exact solution

[{x'=-x, y'=y/2}]x*y^2 = 1

- Ghost variable solution needs to exist for at least as long as original diffeq

Pros/Cons of KeYmaera X ODE Tactics

Actual Solution

- Easy to prove things knowing exact solution

{x’ = a}

- Not always easy to find or even represent solutions

{x’ = x}

Differential Invariant

- Analyze trends in how quantities change without knowing exact solution

[{x’=-y, y’=x}] x^2+y^2 = 1

- Trends may not help in proof

[{x’=-x}]x > 0

Differential Ghost

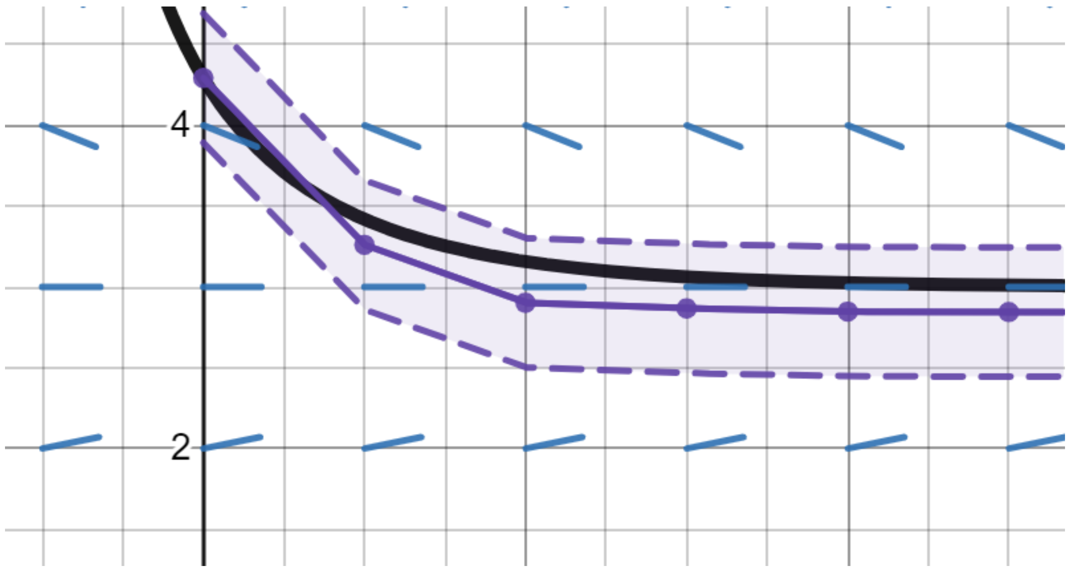
- Use ghost variable to analyze how quantities change without knowing exact solution

[{x’=-x, y’=y/2}]x*y^2 = 1

- Ghost variable solution needs to exist for at least as long as original diffeq

Numerical methods can offer approximate solutions which are almost like actual solutions

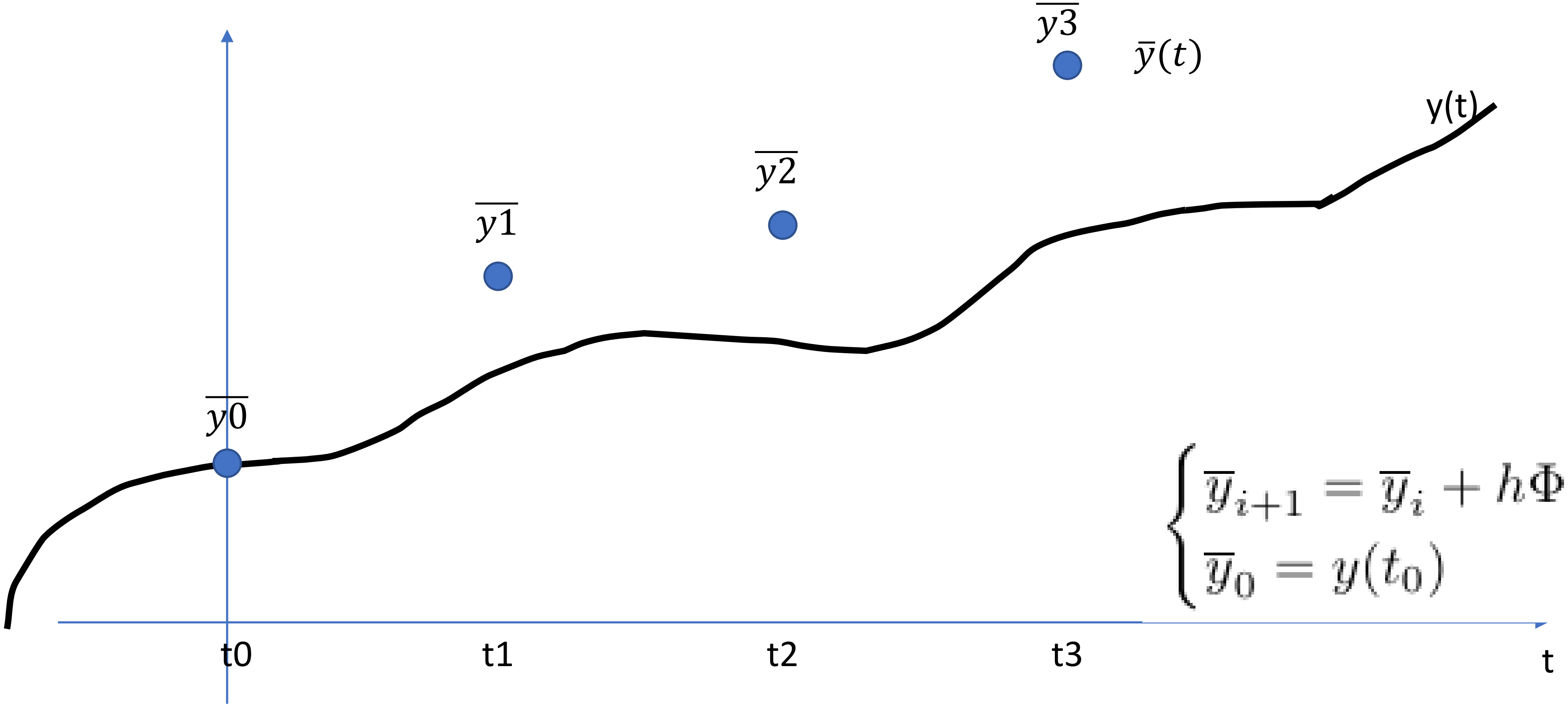
- Require timestep specification
- Symbolic initial value problem
- How to transform post conditions to account for error



$$\begin{cases} \overline{y}_{i+1} = \overline{y}_i + h\Phi(t_i, \overline{y}_i | h) \\ \overline{y}_0 = y(t_0) \end{cases}$$

Theory: constructing approximations

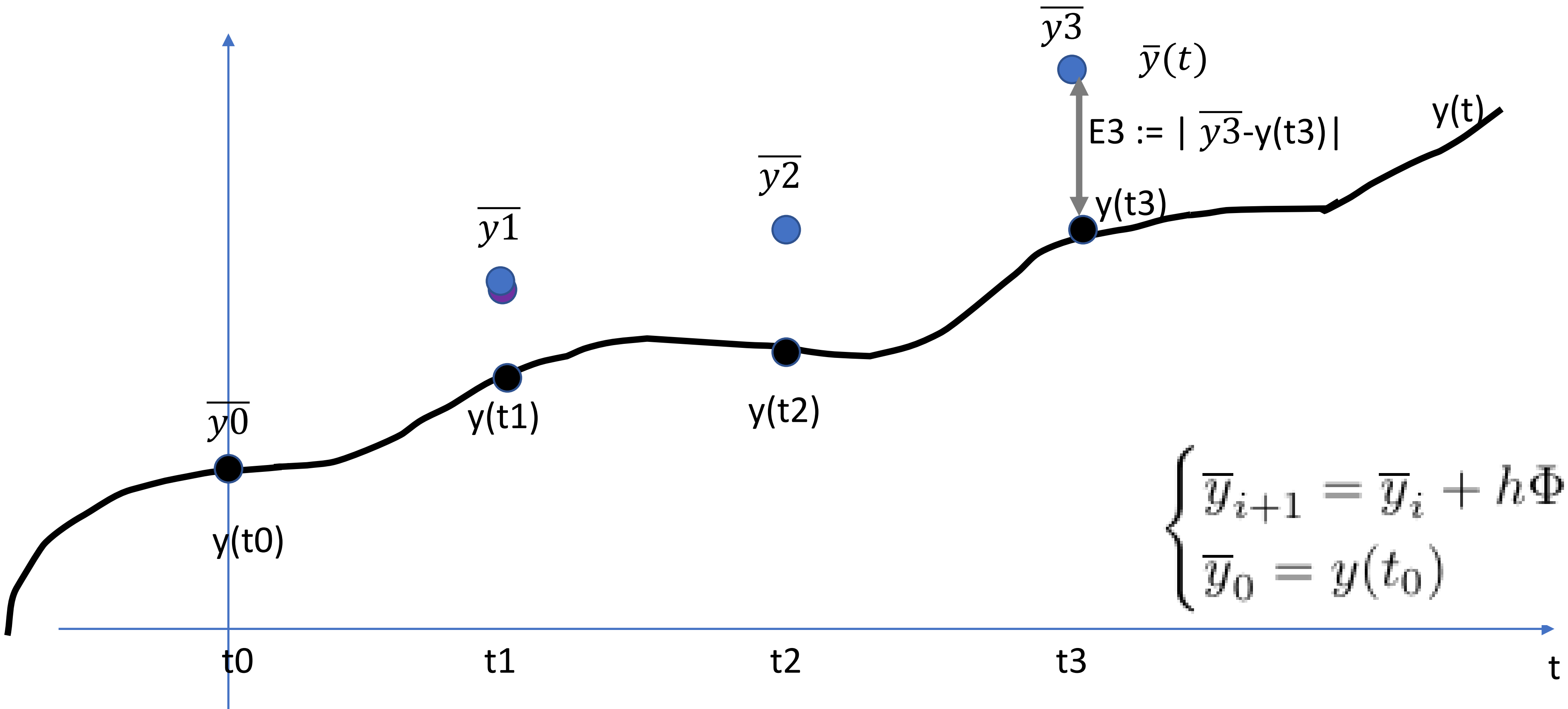
- Given timestep h, numerical methods can yield discrete approximations



$$\begin{cases} \overline{y}_{i+1} = \overline{y}_i + h\Phi(t_i, \overline{y}_i | h) \\ \overline{y}_0 = y(t_0) \end{cases}$$

Theory: global error of discrete approximation

Define error Ei := | $\overline{yi} - y(ti)$|, want to find global bound on error

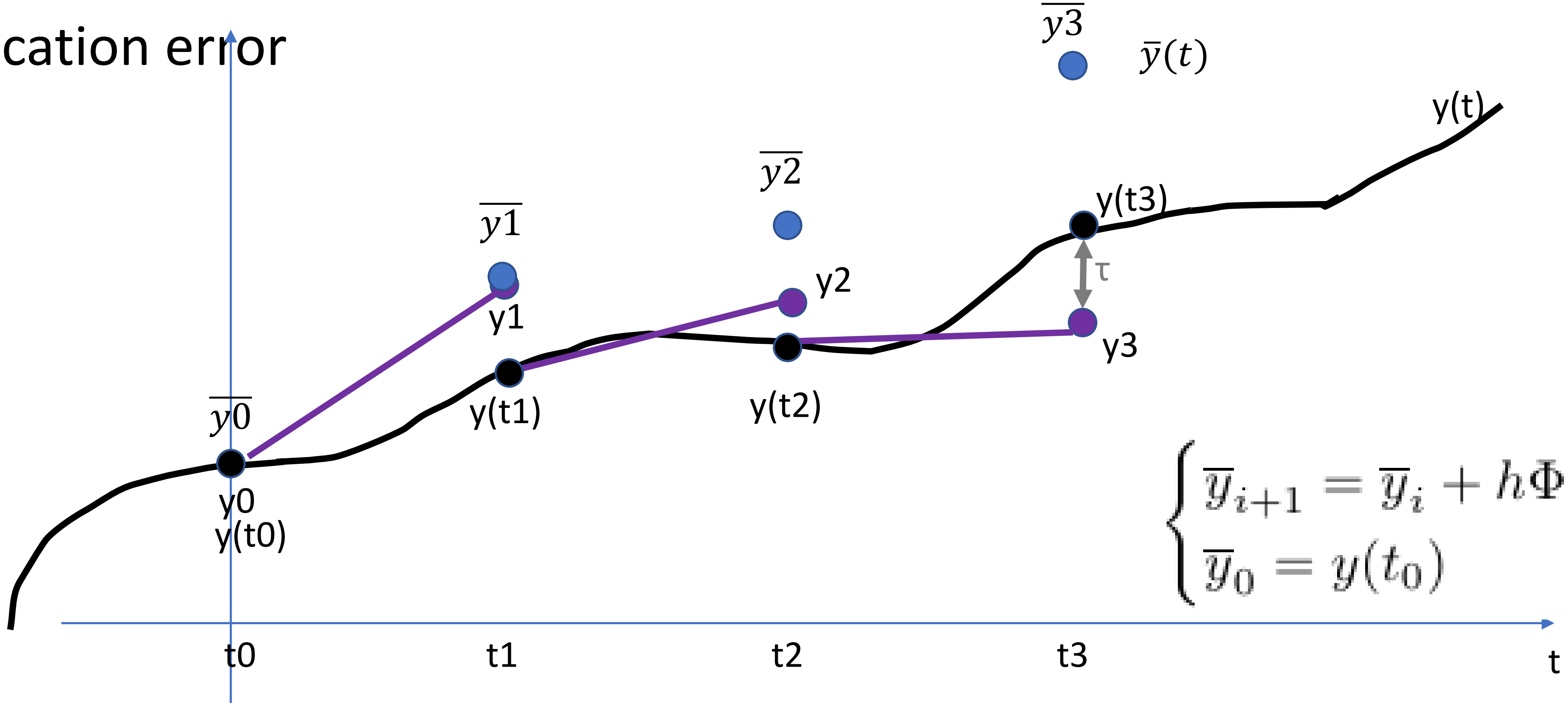


$$\begin{cases} \overline{y}_{i+1} = \overline{y}_i + h\Phi(t_i, \overline{y}_i | h) \\ \overline{y}_0 = y(t_0) \end{cases}$$

Theory: global error of discrete approximation

Introduce new sequence {y(i+1) = $y(t_i) + h\Phi(t_i, y(t_i)|h)$} (one step) approximations

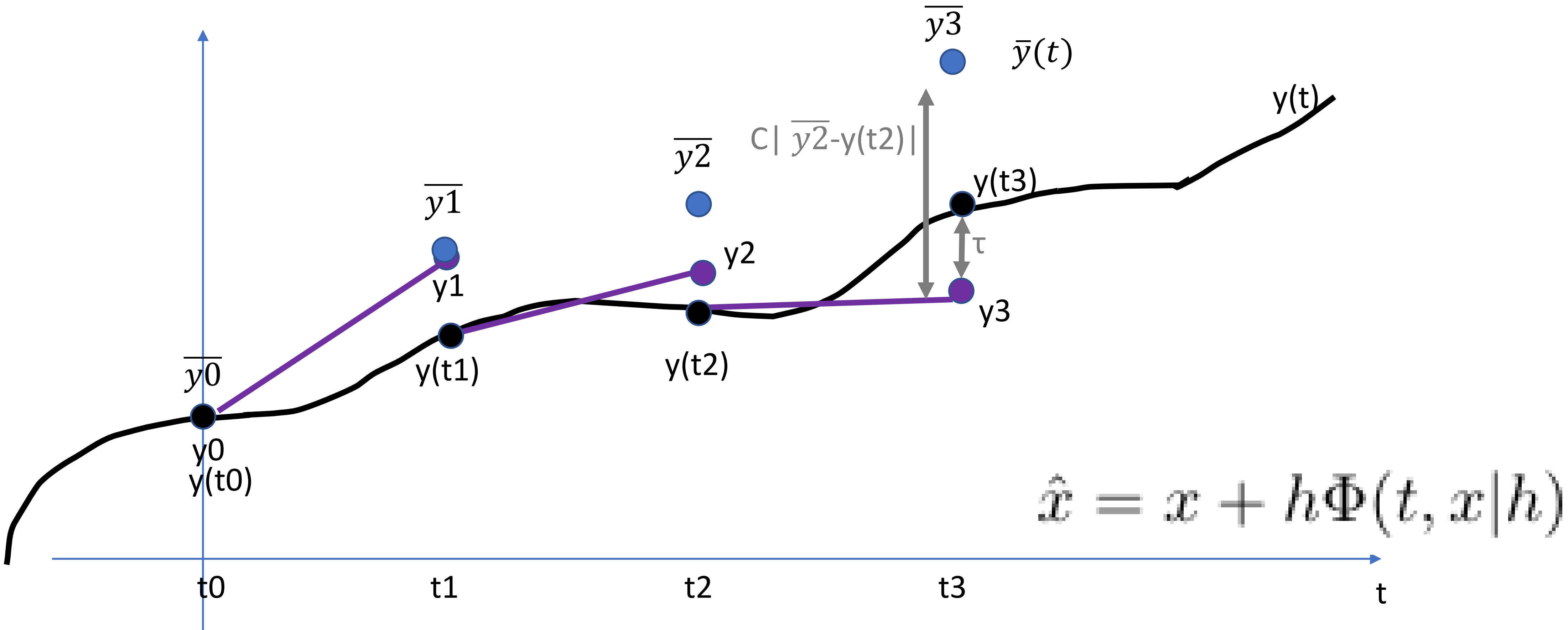
Truncation error



$$\begin{cases} \overline{y}_{i+1} = \overline{y}_i + h\Phi(t_i, \overline{y}_i|h) \\ \overline{y}_0 = y(t_0) \end{cases}$$

Theory: global error of discrete approximation

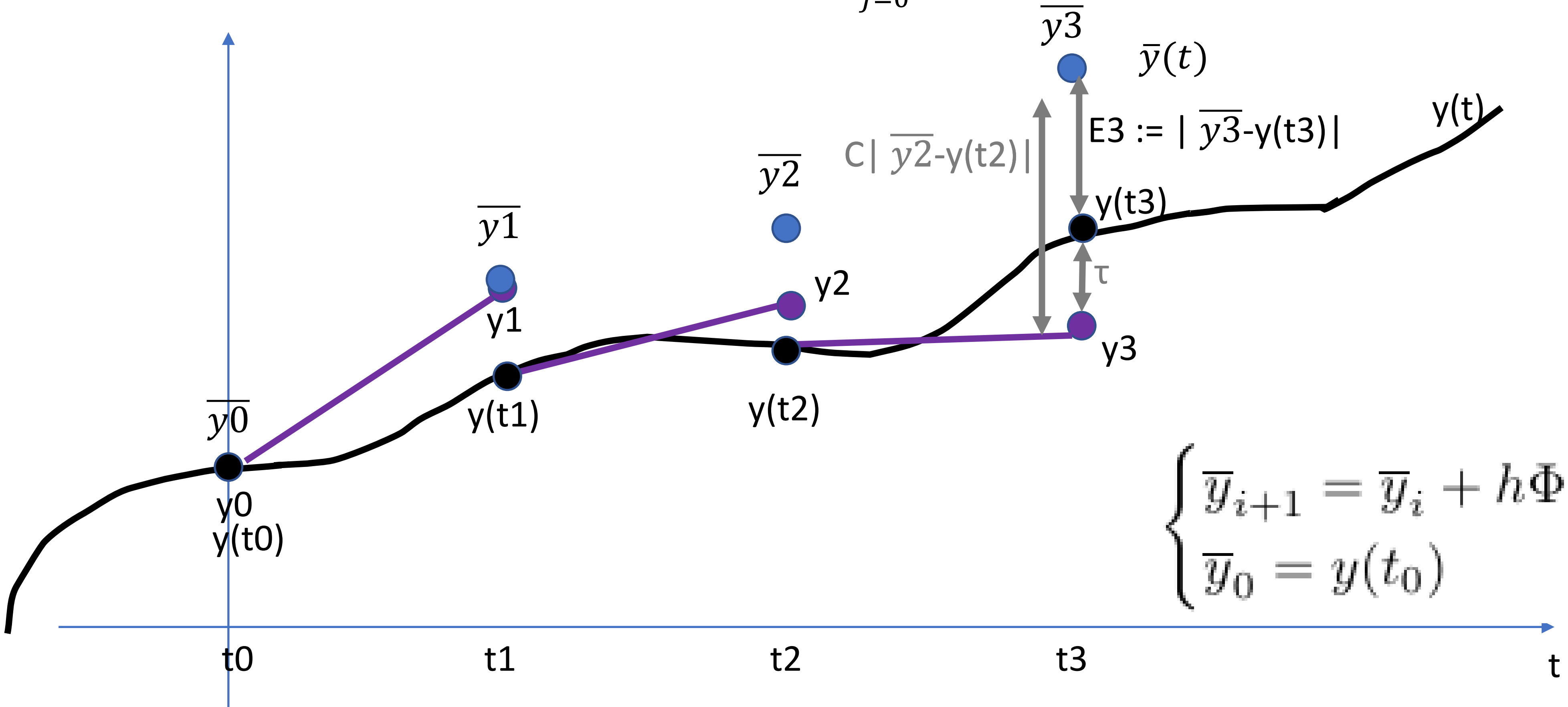
If ϕ sufficiently nice, exists constant C such that $|\hat{y} - \hat{z}| \leq |y - z|C$



Theory: global error of discrete approximation

If N=T/h, global error of discrete approximation

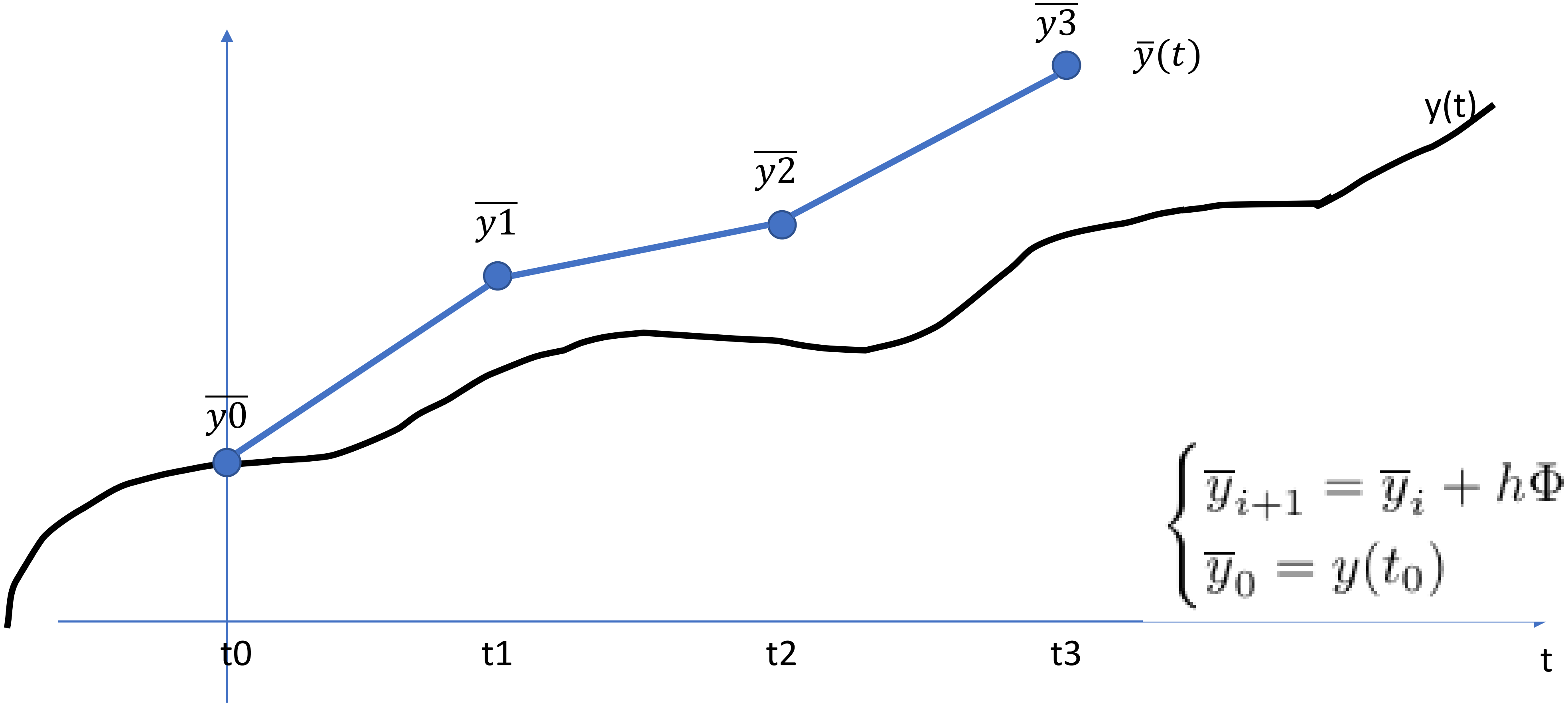
$$E_{i+1} \leq CE_i + \tau \ \leq C^{i+1}E_0 + \tau \sum_{j=0}^{i-1} C^j \leq \tau \frac{C^N - 1}{C - 1}$$



$$\begin{cases} \overline{y}_{i+1} = \overline{y}_i + h\Phi(t_i, \overline{y}_i | h) \\ \overline{y}_0 = y(t_0) \end{cases}$$

Theory: constructing approximations

- Use linear interpolation to convert to continuous approximations

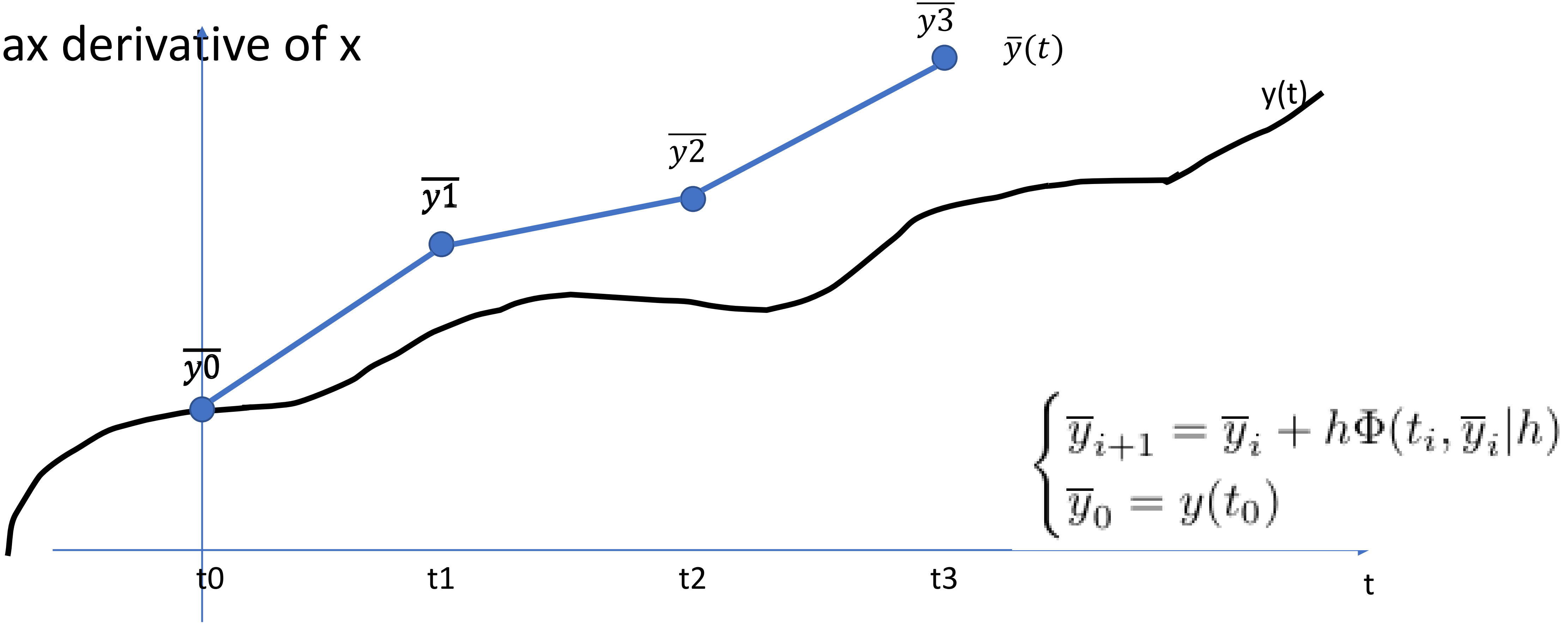


$$\begin{cases} \overline{y}_{i+1} = \overline{y}_i + h\Phi(t_i, \overline{y}_i | h) \\ \overline{y}_0 = y(t_0) \end{cases}$$

Theory: global error of continuous approximation

If ϵ_a is discrete approximation error, then continuous approximation error of linear interpolation is bounded by ϵ_a+hL

L: max derivative of x



Theory: global error

global error of continuous approximation
ϵ_a +hL

global error of discrete approximation

$$\epsilon_a \leq \tau \frac{C^N - 1}{C - 1}$$

Putting it together

If desired error bound is ϵ,

Solve for h

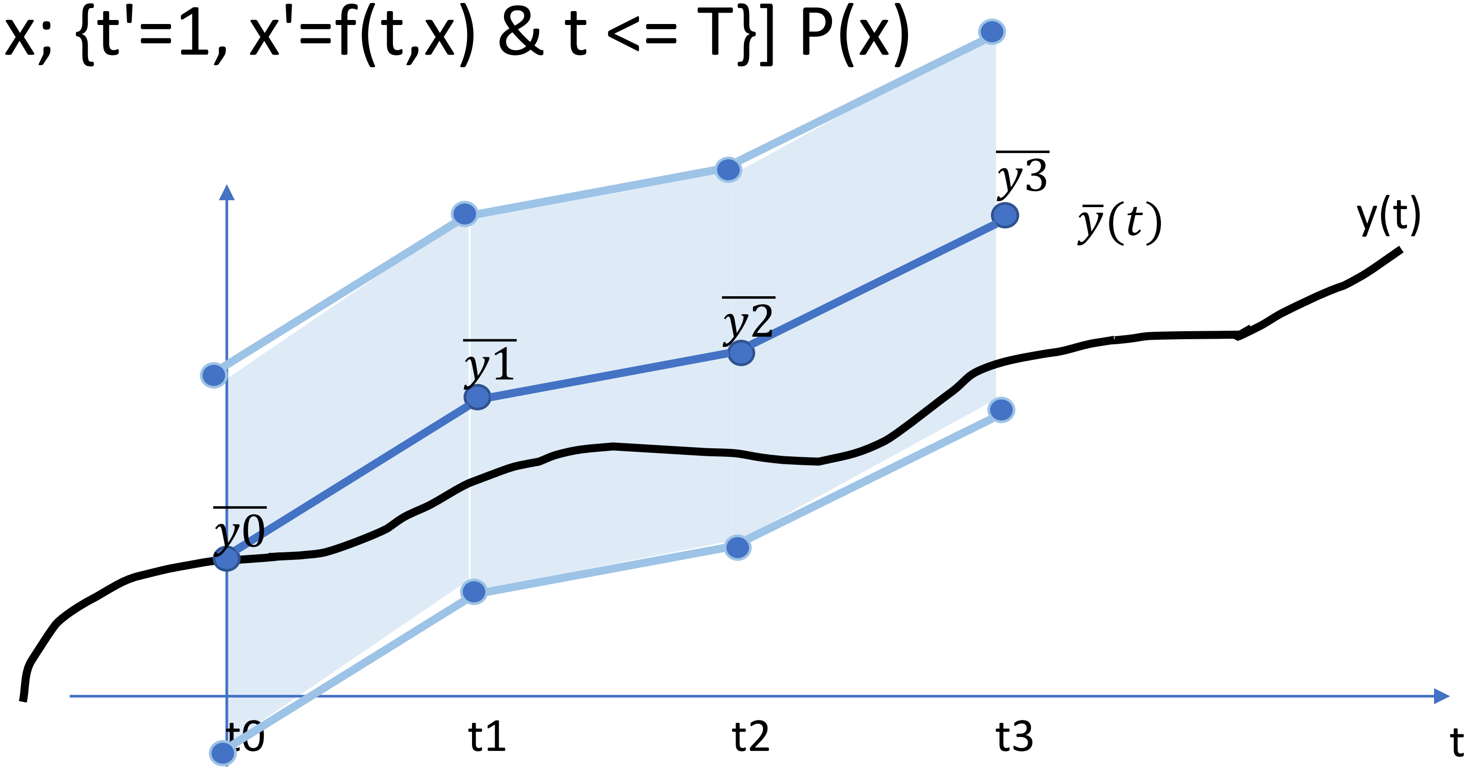
$$\epsilon = \tau \frac{C^N - 1}{C - 1} + hL$$

Theory: Proof Rule

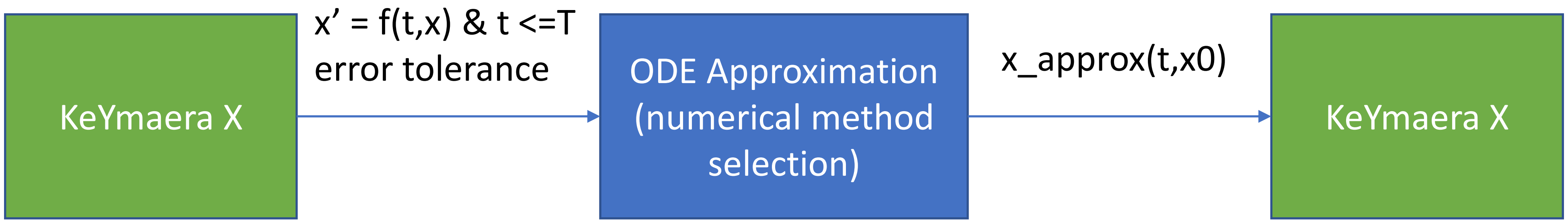
\exists e > 0 \forall t (0 <= t <= T & |x-x_approx(x0,t,eps)| < e -> P(x))

-- [dApprox]

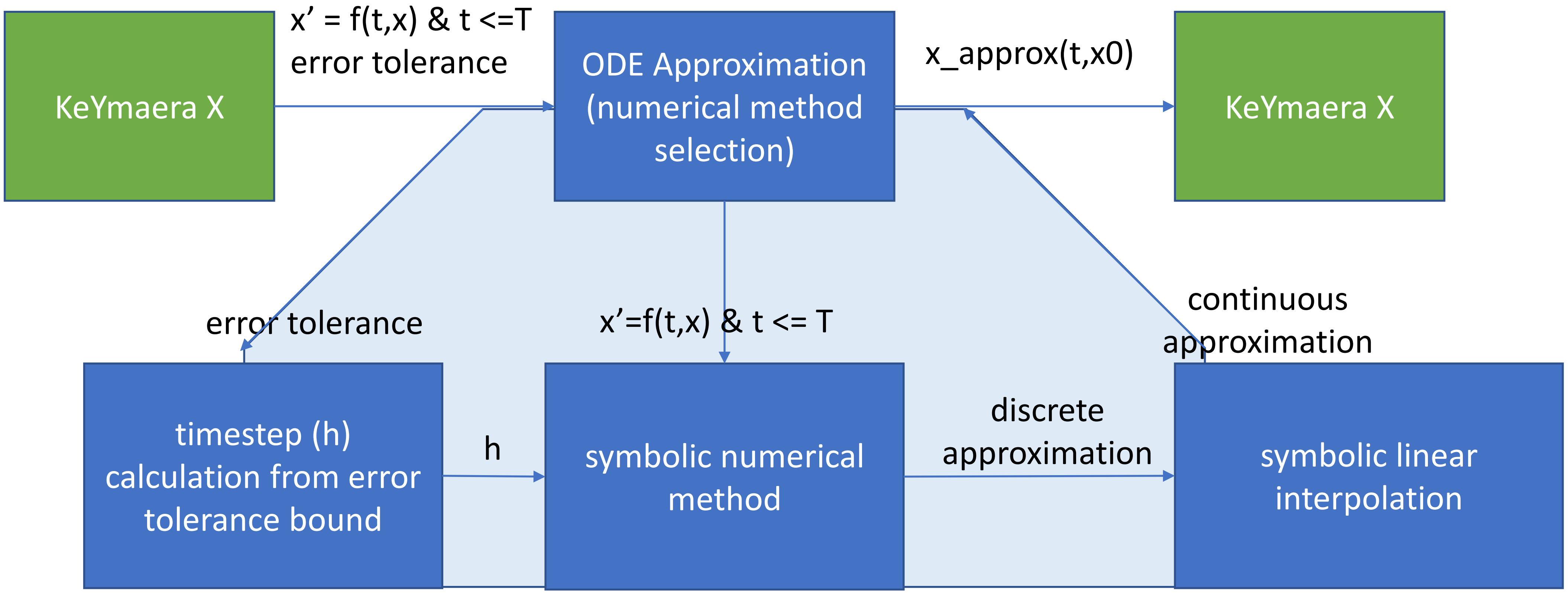
[t:=0; x0 := x; {t'=1, x'=f(t,x) & t <= T}] P(x)



Implementation:



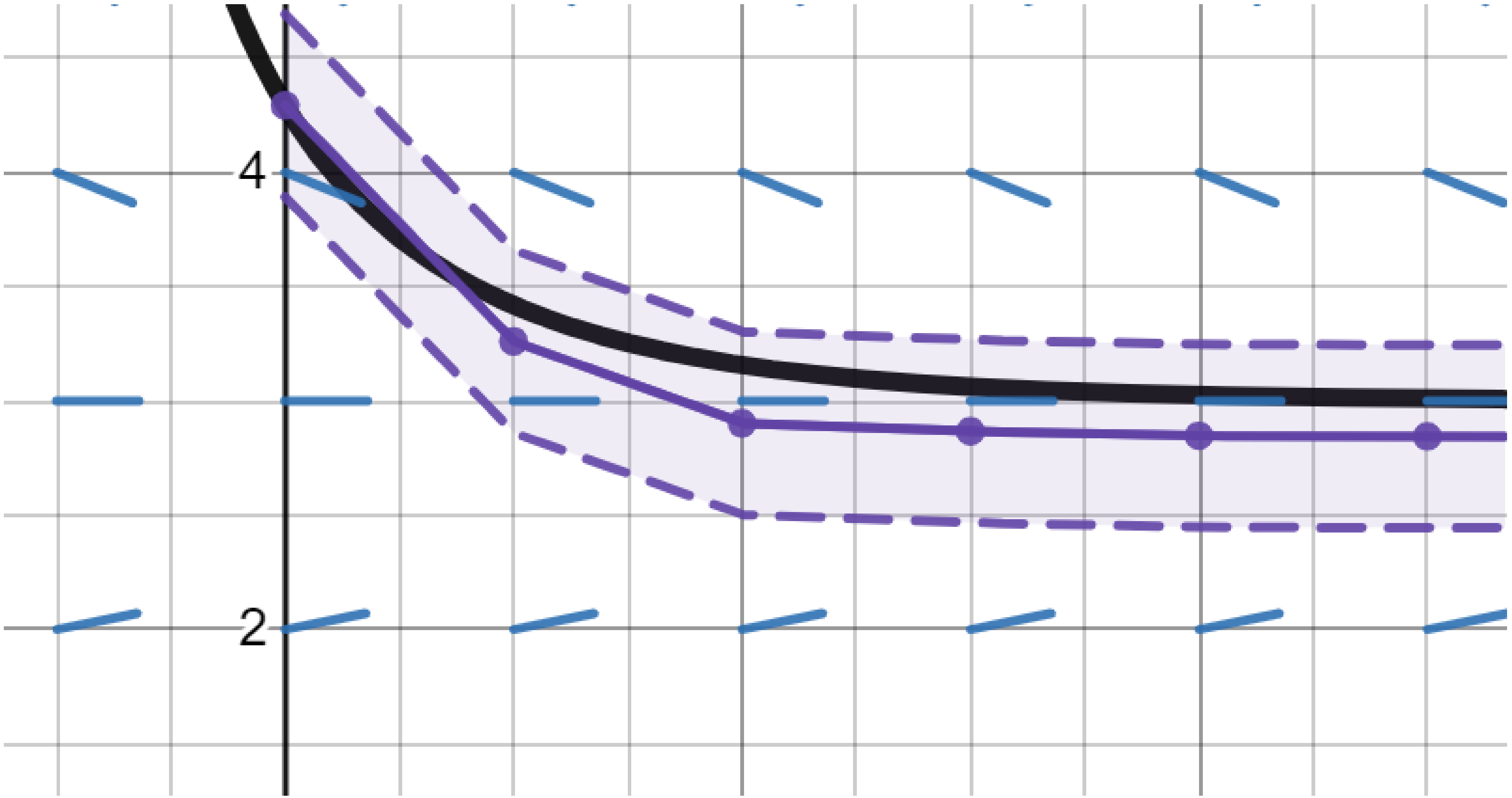
Implementation:



Discussion and Further Work

- Comparison of existing KeYmaera X tools for analyzing ODEs
- Theory of how to convert desired error tolerance into continuous approximation
- Implementation

- Convert python function into KeYmaera X function
- Handle non-initial value symbols in function $x'=f(t,x)$
- Extend to other numerical methods


4
2