On the Soundness of Behavioural Abstraction in Hybrid Systems

SIM@SYST.Level, 19th of October, 2014, Cargèse, France

Simon Bliudze and Sébastien Furic

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Siemens PLM Software

Towards ~~On~~ the Soundness of Behavioural Abstraction in Hybrid Systems

SIM@SYST.Level, 19th of October, 2014, Cargèse, France

Simon Bliudze and Sébastien Furic

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Siemens PLM Software

SIEMENS

LMS ENGINEERING INNOVATION

Towards

~~On~~ the Soundness of Behavioural Abstraction in Hybrid Systems

S. Bliudze and S. Furic. *An Operational Semantics for Hybrid Systems Involving Behavioral Abstraction*. Proc. of the 10th International Modelica Conference, Lund, Sweden, pp. 693–706. 2014.

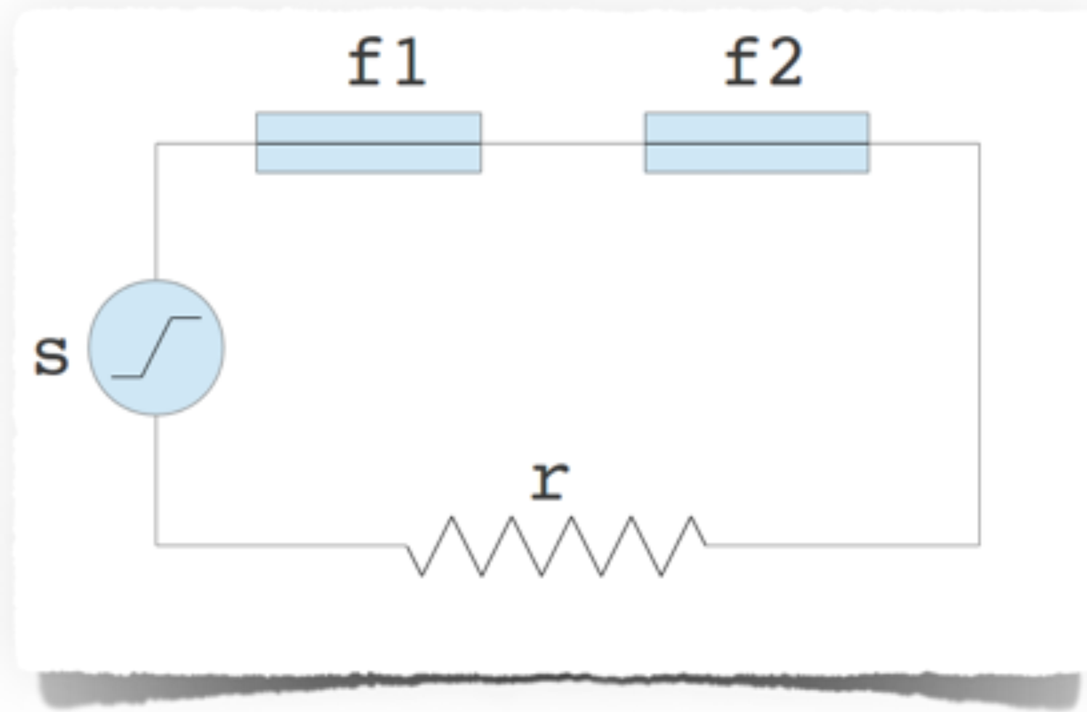
Simon Bliudze and Sébastien Furic

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Siemens PLM Software

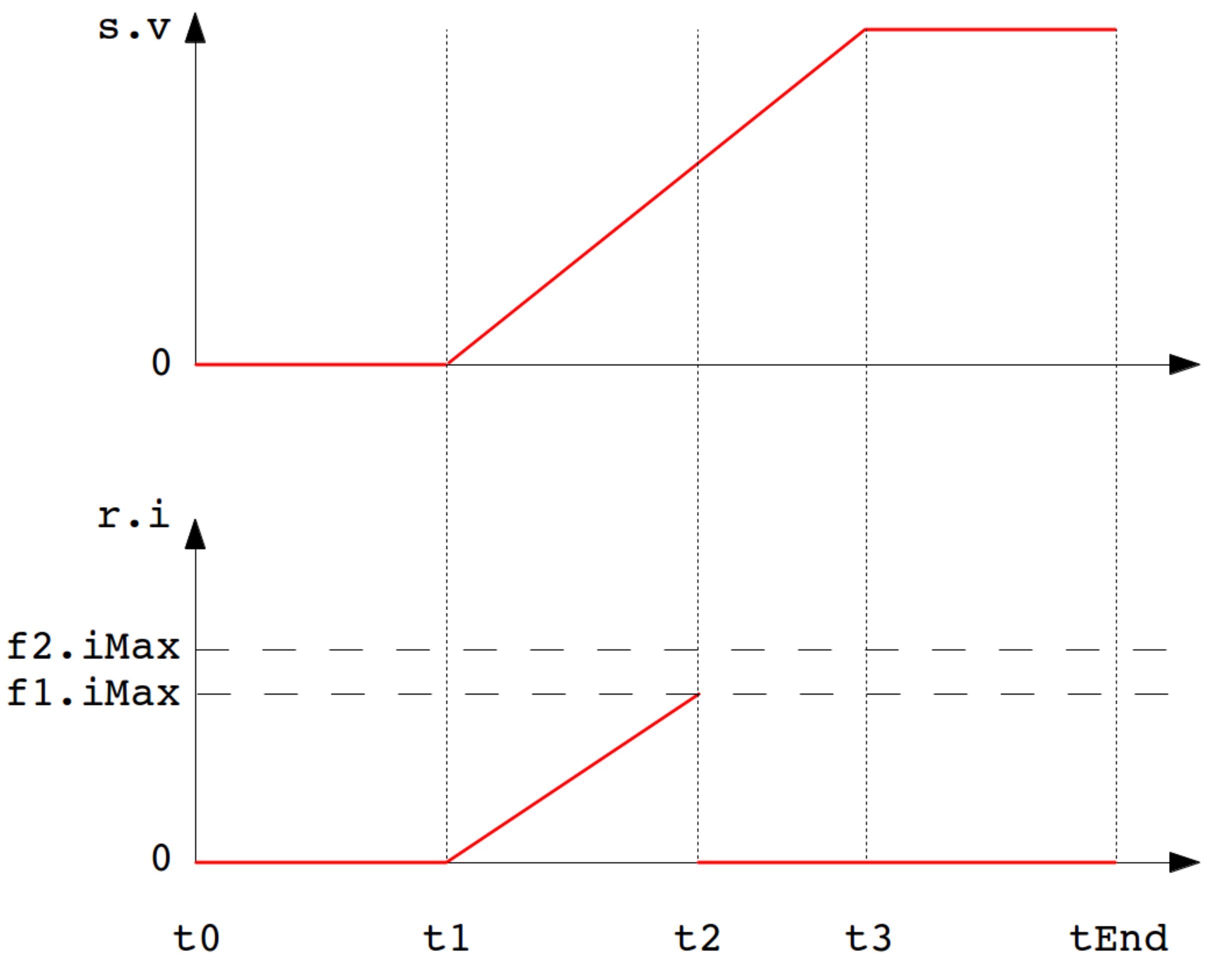
Abstraction

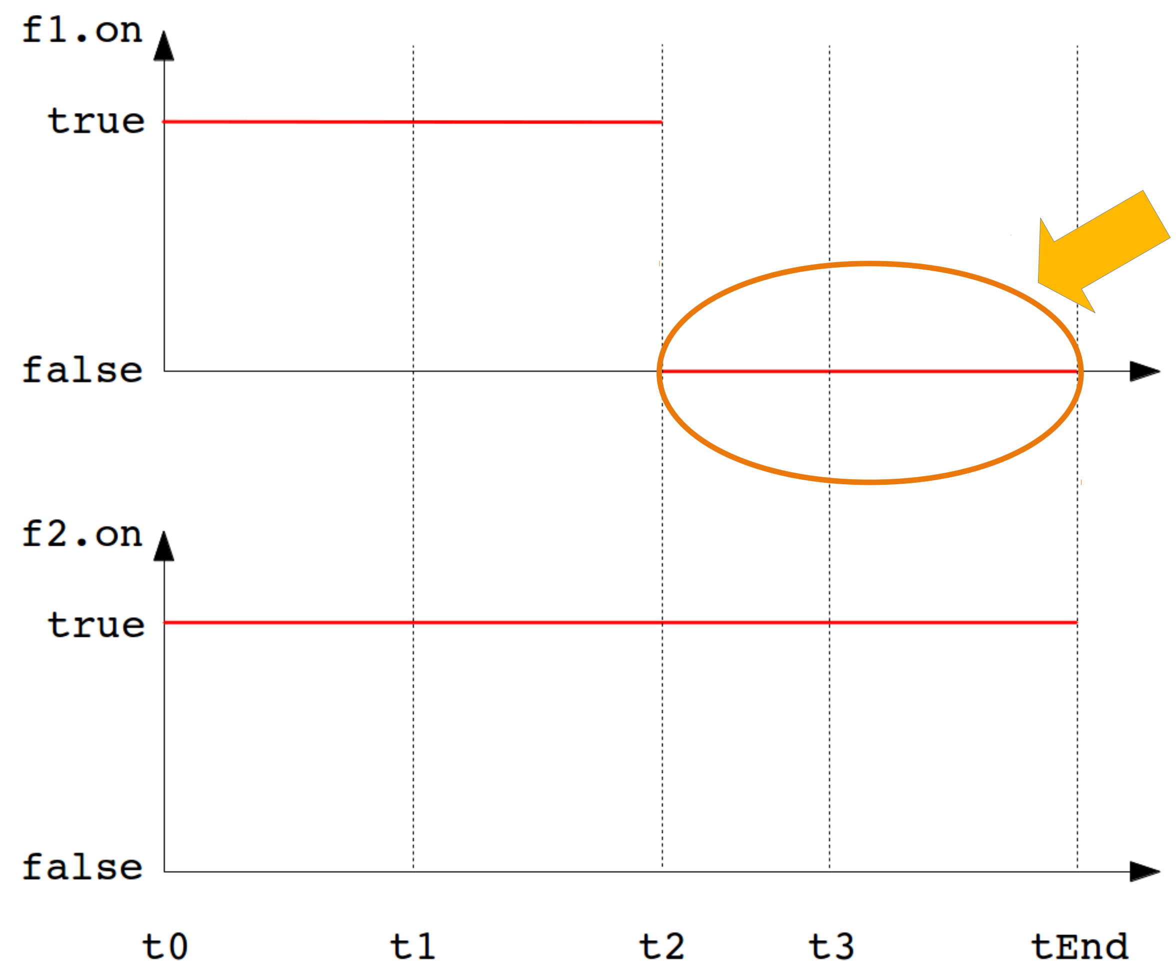
```
model Fuse
    extends Interfaces.OnePort;
    parameter Real iMax;
    parameter Real Ron, Roff;
    Boolean on;
protected Real R;
initial equation
    on = true;
equation
    when i > iMax then
        on = false;
    end when;
    R = if on then Ron else Roff;
    v = R * i;
end Fuse;
```



- The fuse model assumes negligible melting duration
    - In particular w.r.t. the raise duration of the voltage source

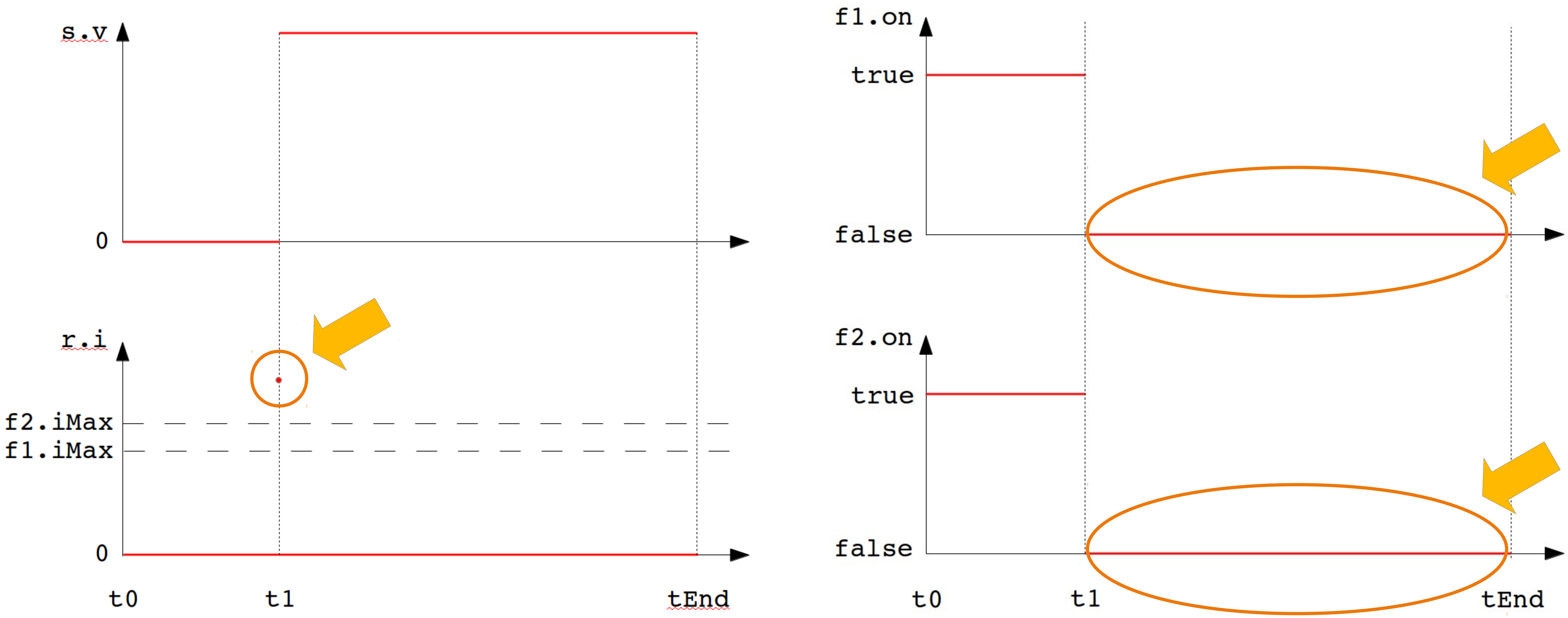
Expected behaviour





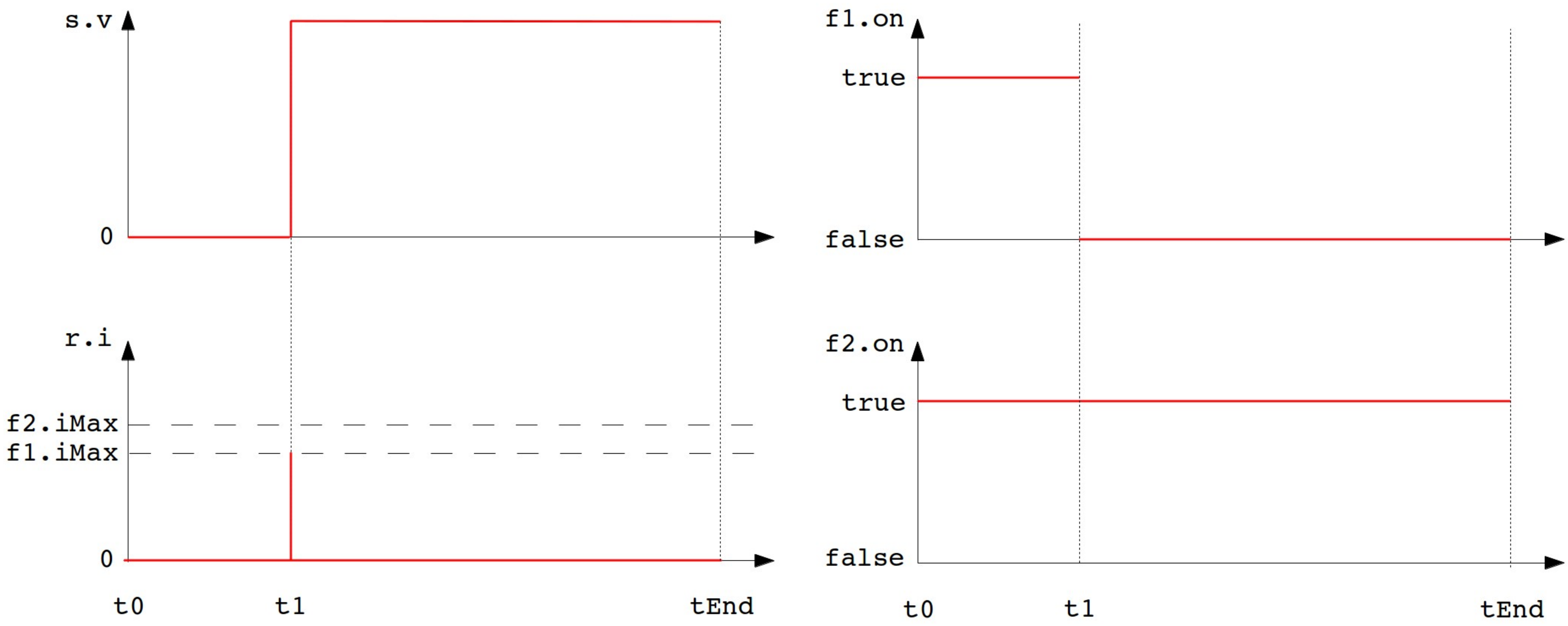
- Only the first fuse melts
  - Independently of the voltage slope

Nested abstraction



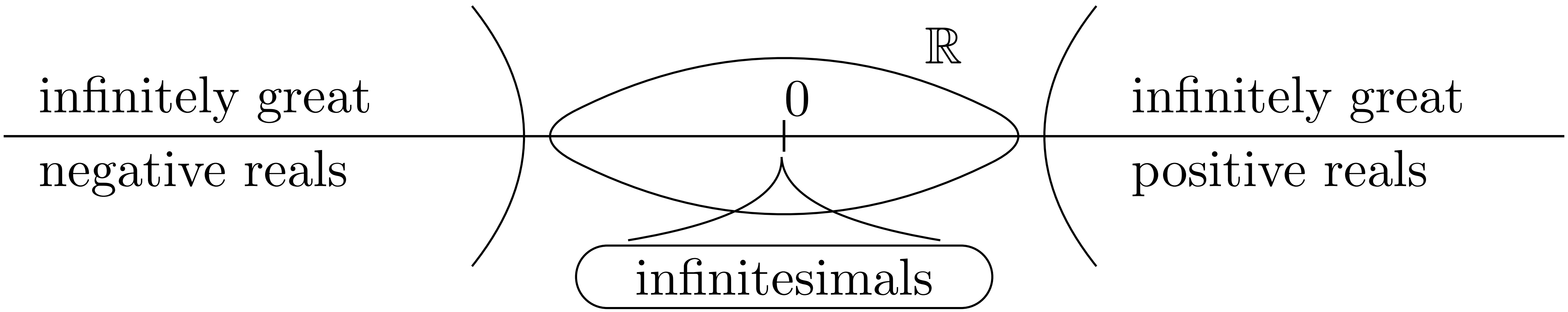
- Suppose we **also** abstract the behaviour of the voltage source
- Both fuses melt due to the loss of signal continuity

Desired behaviour



- Signals are no longer maps from time to values
- We need **infinitesimal** time steps to enable this behaviour

Non-standard analysis



- Used **intuitively** by Leibniz and Newton
- Formalised by Abraham Robinson in the 60s

$$N, N+1, N^2, N/2, e^N, \ldots \qquad \varepsilon = 1/N, \ldots \qquad \varepsilon \approx 0$$

Standardisation

- Every finite non-standard real has a unique standard part

$$x = \mathrm{std}(x) + \varepsilon \qquad \mathrm{std}(x) \in \mathbb{R} \qquad \varepsilon \approx 0$$

- Functions can be standardised

$$\forall x \in \mathbb{R},\ \mathrm{std}\big(f\big)(x) \stackrel{def}{=} \mathrm{std}\big(f(x)\big)$$

- Standardisation of a function is **not** defined on all non-standard reals, but only on the standard ones

$$f : {}^*\mathbb{R} \to {}^*\mathbb{R} \qquad \mathrm{std}\big(f\big) : \mathbb{R} \to \mathbb{R}$$

Examples

- Differentiation

$$\frac{d\left(x^2\right)}{dx} = \frac{(x+dx)^2 - x^2}{dx} = \frac{2x\,dx + dx^2}{dx} = 2x + dx \approx 2x$$

- Integration

$$\int_0^1 f(x)dx \approx \sum_{i=0}^{N-1} f(i\,dx)dx\,,\ \text{where } N = 1/dx$$

- Continuity

$$\forall x \in {}^*\mathbb{R}, \quad x \approx a \implies {}^*f(x) \approx {}^*f(a)$$

Everything is a sequence

$$1 = [1, 1, 1, \ldots] \qquad {}^*f = [f, f, f, \ldots]$$

$$N = [1, 2, 3, \ldots] \qquad \varepsilon = 1/N = [1, \frac{1}{2}, \frac{1}{3}, \ldots]$$

$$N + 1 = [2, 3, 4, \ldots] \qquad \varepsilon^2 = 1/N^2 = [1, \frac{1}{4}, \frac{1}{9}, \ldots]$$

Quite similar in spirit to the definition of reals using Cauchy sequences

$$x = [x_1, x_2, x_3, \ldots] \qquad y = [y_1, y_2, y_3, \ldots]$$

$$x < y \overset{def}{\Longleftrightarrow} x_i < y_i \text{ for almost all } i$$

Everything is a sequence

$$1 = [1, 1, 1, \ldots]$$

$$N = [1, 2, 3, \ldots]$$

$$N + 1 = [2, 3, 4, \ldots]$$

$$^*f = [f, f, f, \ldots]$$

$$\varepsilon = 1/N = [1, \frac{1}{2}, \frac{1}{3}, \ldots]$$

$$\varepsilon^2 = 1/N^2 = [1, \frac{1}{4}, \frac{1}{9}, \ldots]$$

Quite similar in spirit to the definition of reals using Cauchy sequences

$$x = [x_1, x_2, x_3, \ldots] \qquad y = [y_1, y_2, y_3, \ldots]$$

$$x < y \overset{def}{\iff} x_i < y_i \text{ for almost all } i$$

Transfer principle

- Non-standard reals are a **first-order equivalent** model of the real field
  - Any first-order formula true in $\mathbb{R}$ is true in $^*\mathbb{R}$ and vice-versa.

- Example (continuity):

$$\forall \varepsilon \in \mathbb{R}(\varepsilon > 0), \exists \delta \in \mathbb{R}(\delta > 0) : \quad \forall x \in \mathbb{R}, \big(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon\big)$$

Transfer principle

- Non-standard reals are a **first-order equivalent** model of the real field
  - Any first-order formula true in $\mathbb{R}$ is true in ${}^*\mathbb{R}$ and vice-versa.
- Example (continuity):

$$\forall \varepsilon \in \mathbb{R}(\varepsilon > 0), \exists \delta \in \mathbb{R}(\delta > 0) : \\ \forall x \in \mathbb{R}, \big(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon\big)$$

$$\forall \varepsilon \in {}^*\mathbb{R}(\varepsilon > 0), \exists \delta \in {}^*\mathbb{R}(\delta > 0) : \\ \forall x \in {}^*\mathbb{R}, \big(|x - {}^*a| < \delta \Rightarrow |{}^*f(x) - {}^*f({}^*a)| < \varepsilon\big)$$

Łoś' theorem

- Generalisation of the transfer principle
  - Any first-order formula is true in ${}^*\mathbb{R}$ if and only if it is true in $\mathbb{R}$ for almost all indices.

- Example (Archimedean property):

$$\varepsilon = [\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots], \forall i \in \mathbb{N}, \varepsilon_i \in \mathbb{R}(\varepsilon_i > 0)$$

$$\forall x \in \mathbb{R}, \exists n \in \mathbb{Z} : \; n\varepsilon_i < x \leq (n+1)\varepsilon_i$$

$$\forall x \in {}^*\mathbb{R}, \exists n \in {}^*\mathbb{Z} : \; n\varepsilon < x \leq (n+1)\varepsilon$$

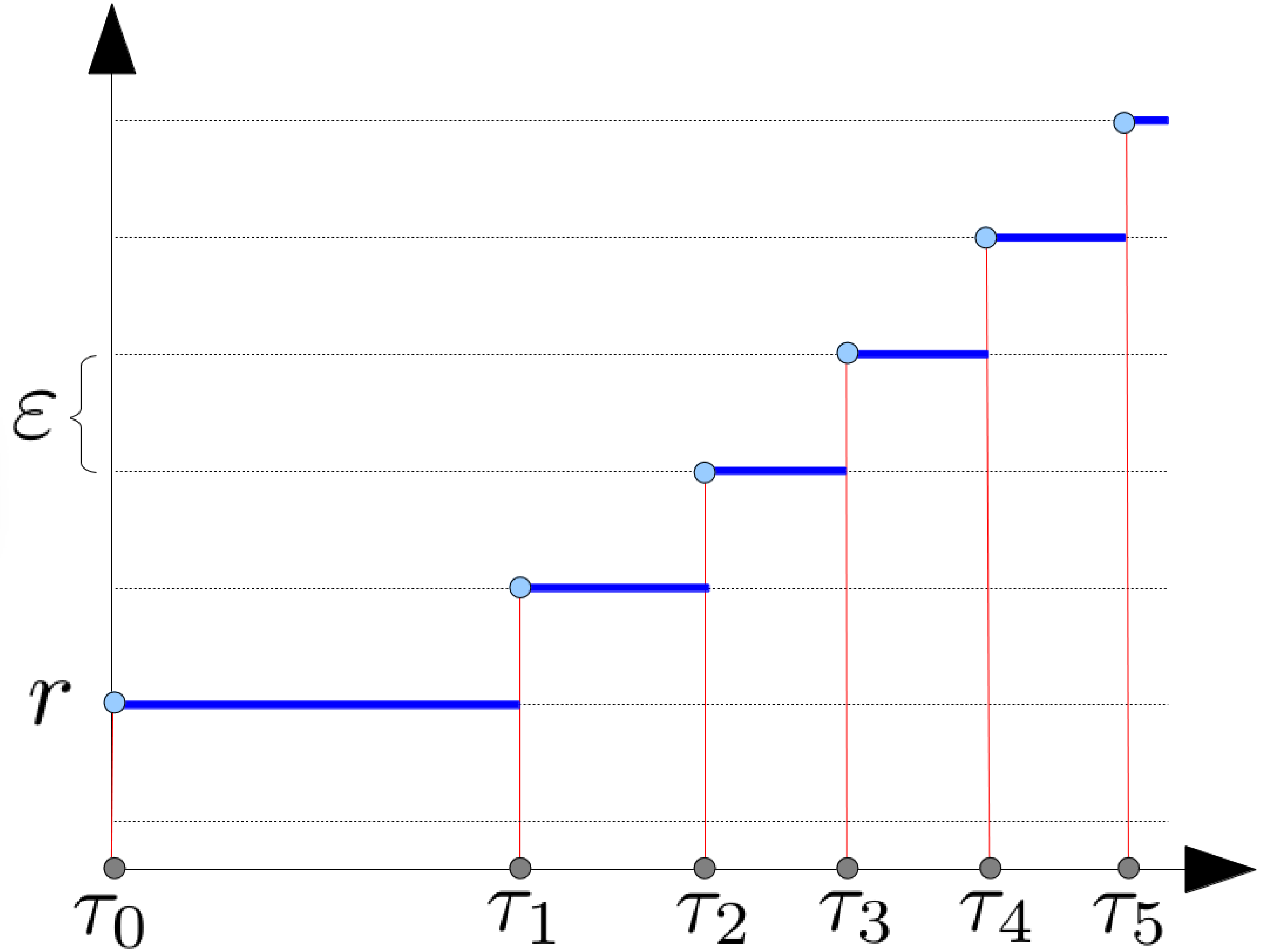
se•man•tic (si man
to meaning or arising from
symbols: semantic change; semantic
semantics. [1655–65; < Gk sēman
mant(ós) marked (sēman-, base o
verbal adj. suffix; akin to sêma si
se•man•tics (si man′tiks), n.
linguistics dealing with the stu
meaning is structured in langu
over time. 2. the branch of s
tionship between signs or s
meaning, or an interpretatio
etc.: Let's not argue
—se•man′ti•

QSS approach

$$^*\mathbb{T} \stackrel{def}{=} {^*\mathbb{R}}_0^+$$

$$^*\mathbb{T} \to r + \varepsilon \cdot {^*\mathbb{Z}}$$

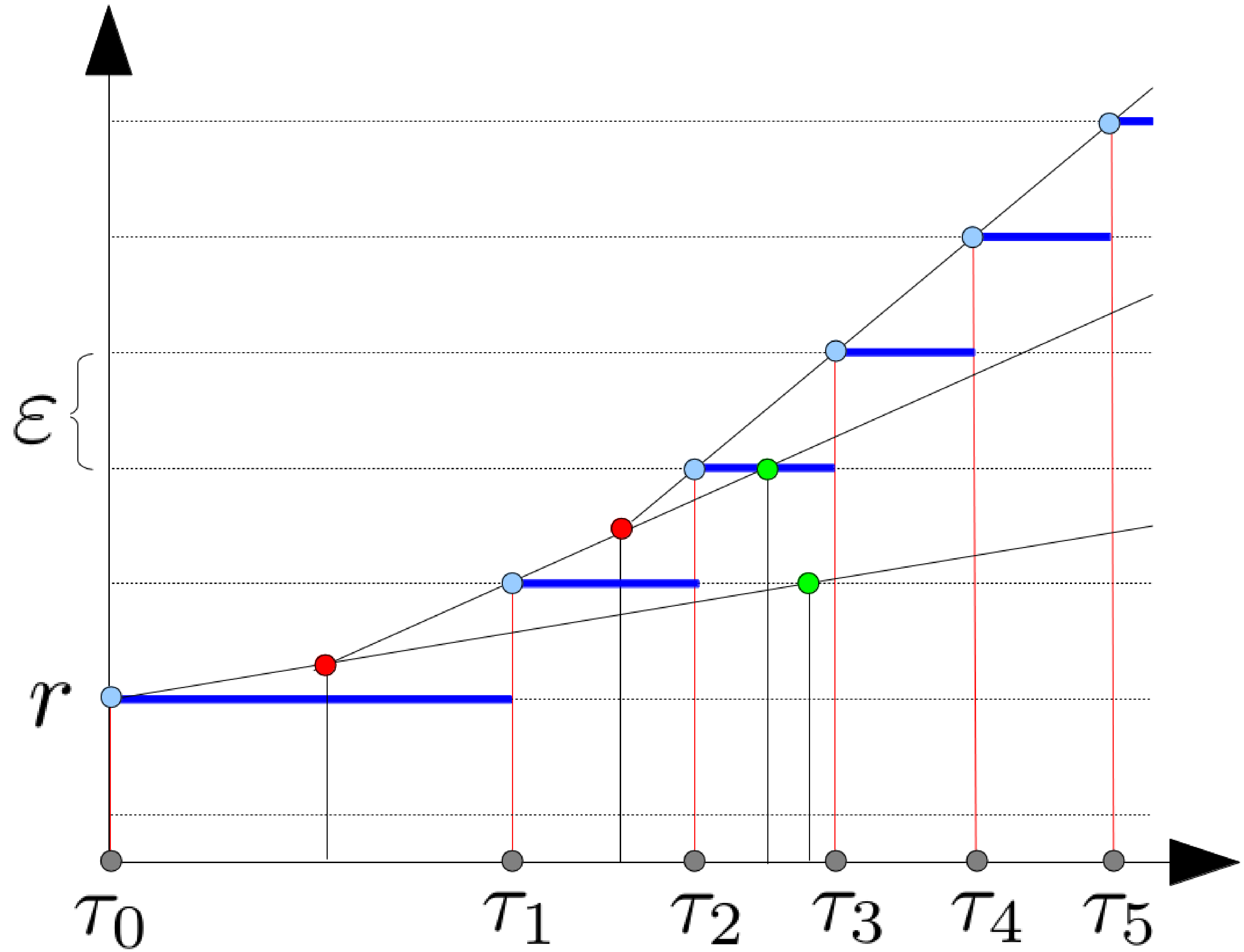
$$\varepsilon \approx 0$$



- Force all dense-time signals to have discrete codomains

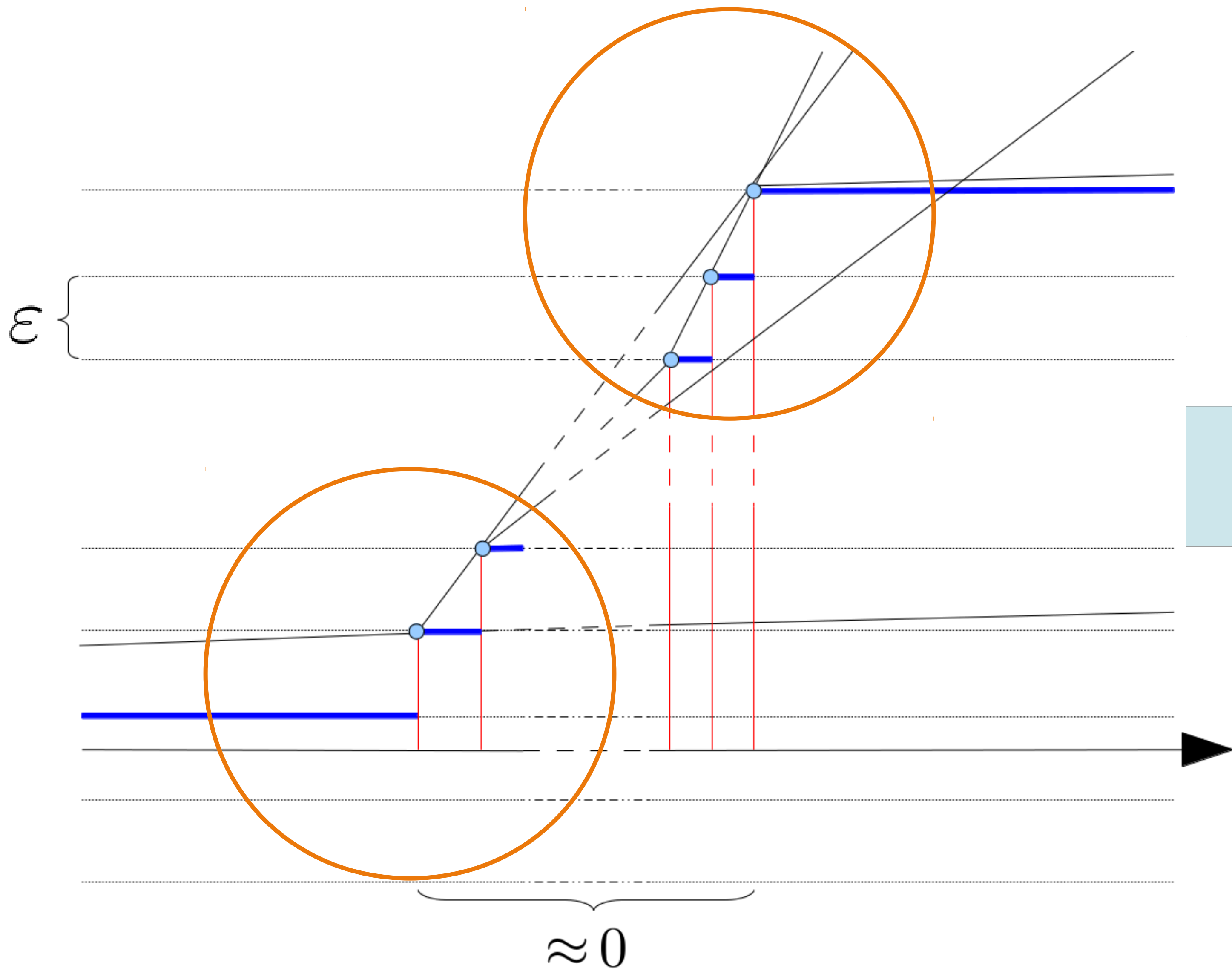
The meaning of ODE

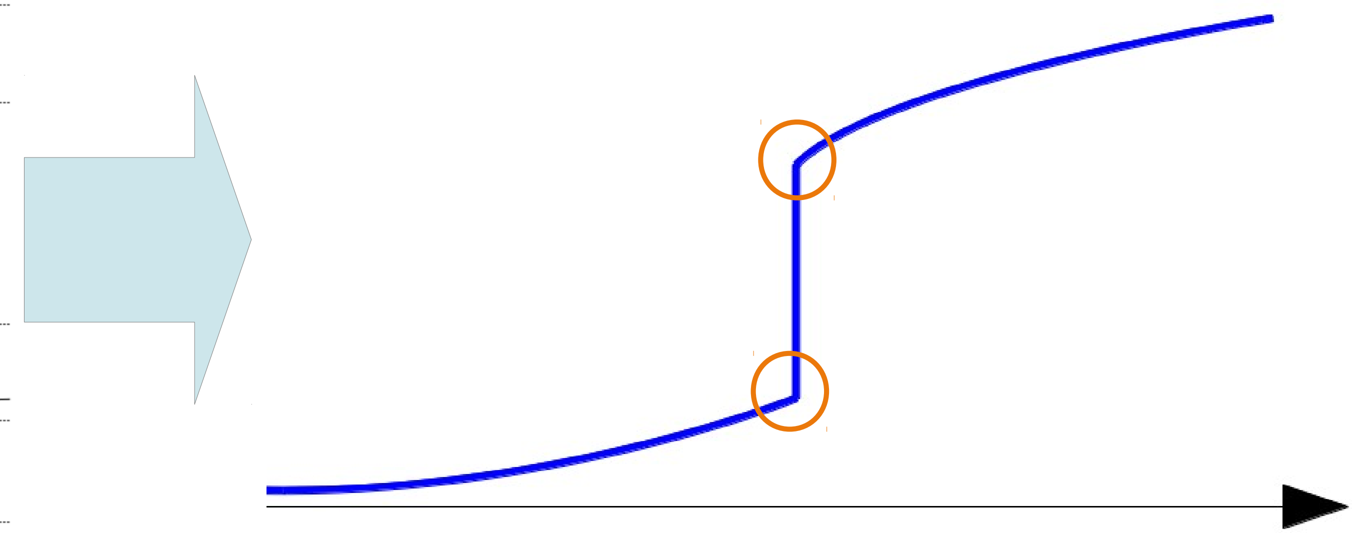
$$\dot{x} = f(x, y)$$
$$x(0) = r$$



- Red dots indicate events on the input signal

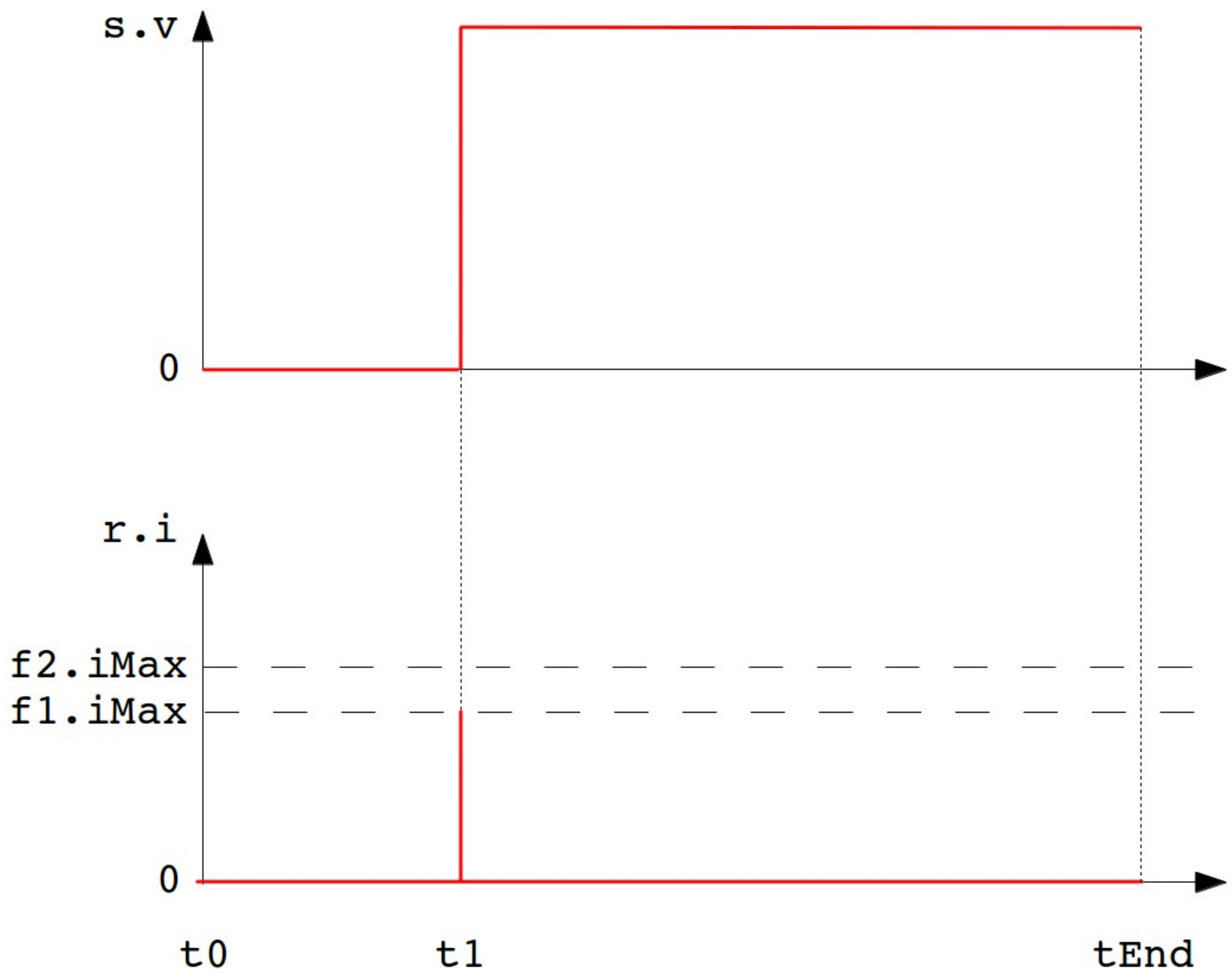
Inifinite slope signals

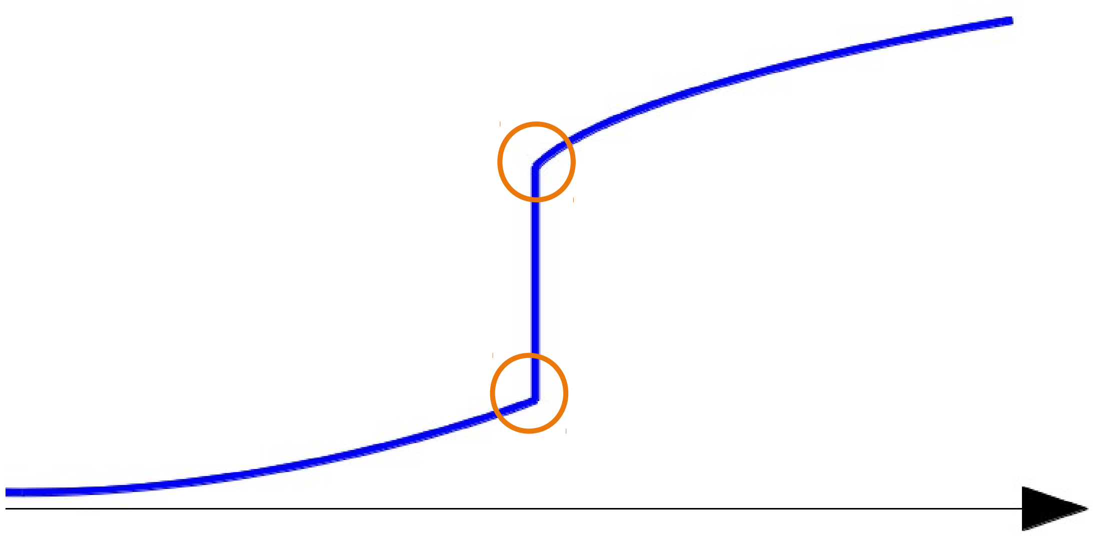




- After “standardisation” they have vertical slopes

Back to the circuit

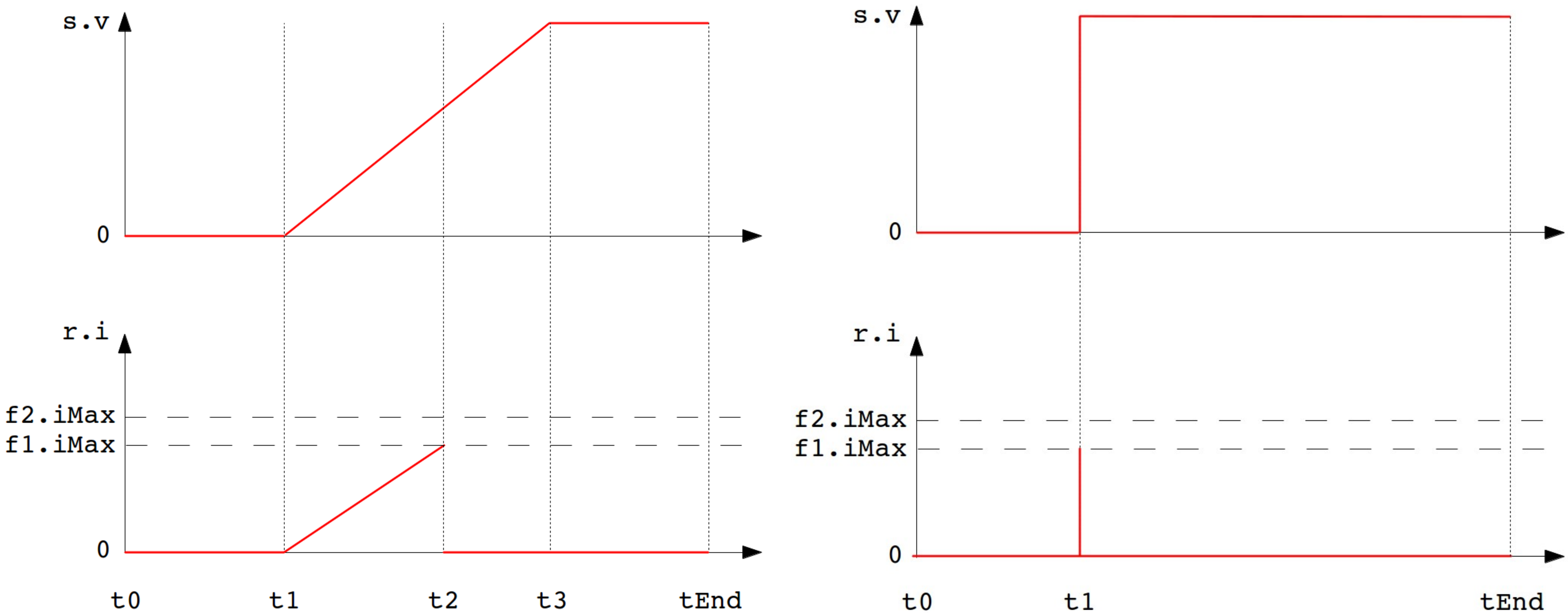




- When the current reaches the rated value of the first fuse, this produces an input event, inverting the slope

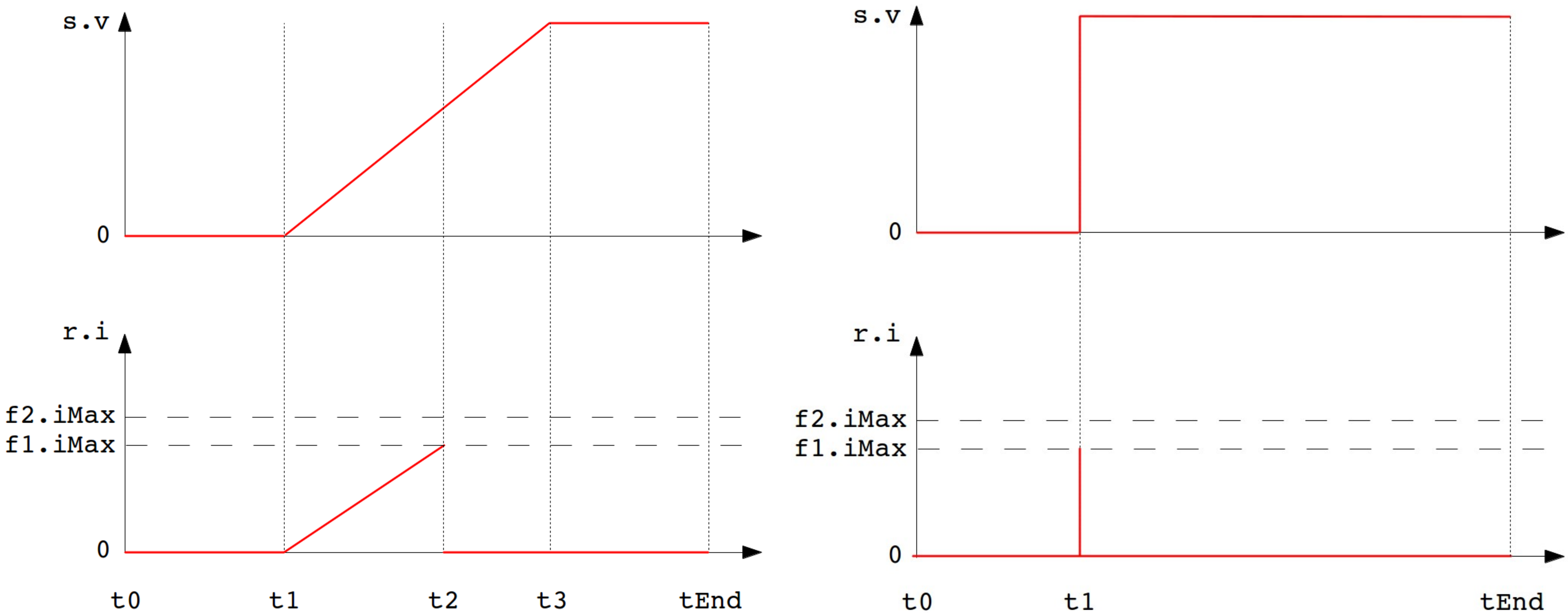

ARE WE THERE YET !?!
MATT GROENING

Key assumptions



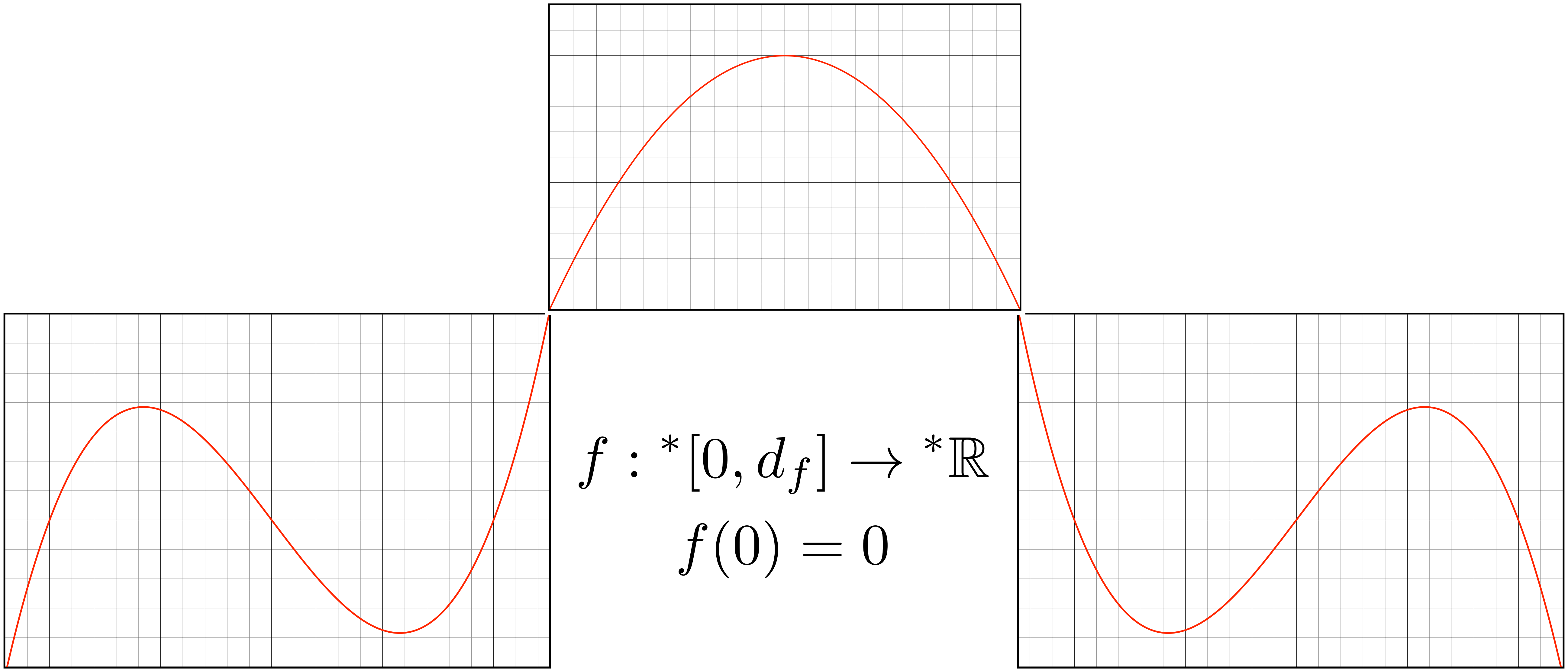
- We rely on two assumptions
  - The signal passes by all intermediate values in the "right order" (continuity)
  - The fuse melts infinitely faster than the voltage increases (model assumption)

Key assumptions



- We rely on two assumptions
  - The signal passes by all intermediate values in the “right order” (continuity)
  - The fuse melts infinitely faster than the voltage increases (model assumption)

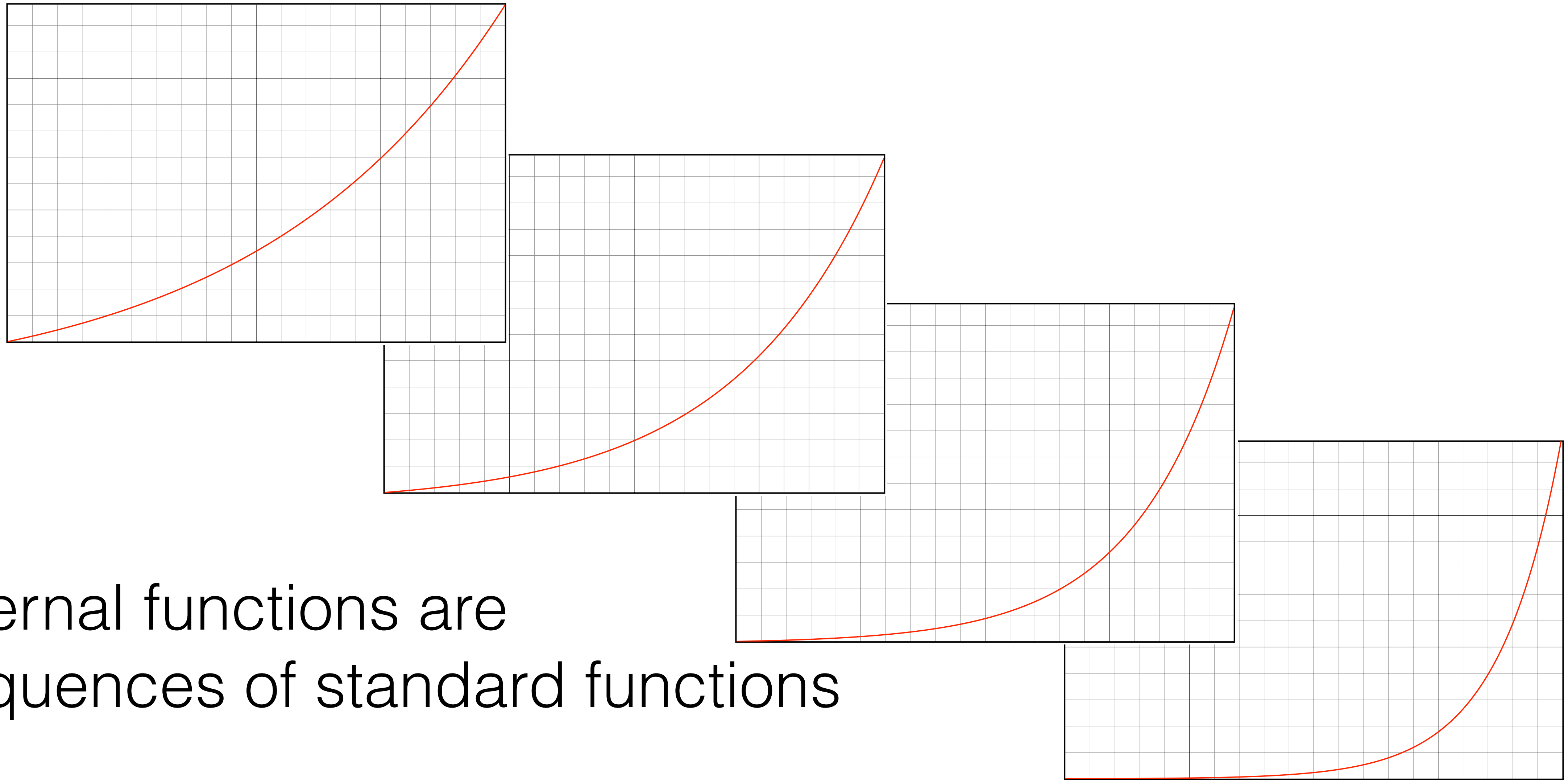
Signets



$$f : {}^*[0, d_f] \to {}^*\mathbb{R}$$
$$f(0) = 0$$

- Consider signals as sequences of additive signets
- A **signet** is a non-standard continuous **internal** function

Specifying abstraction



- Internal functions are sequences of standard functions
- As a consequence of Łoś' theorem, we can reason on standard functions to draw conclusions about the signet
- Use this to derive interval boundaries for the interval abstraction

Conclusion

- We proposed a semantic model for hybrid signals
  - Uniform (linear) and dense nature of time
  - The “physical” properties of signals (read “continuity”)
- Operational, although not directly implementable
  - Describes how to compute the exact solution of a system of dynamic equations
  - Disregarding the finiteness of computational resources
- Can serve as a basis for reasoning and implementation
  - Concrete implementations approximate the solution with non-infinitesimal error
  - New language features can be discussed on a sound basis
- First step towards formalising signal abstraction

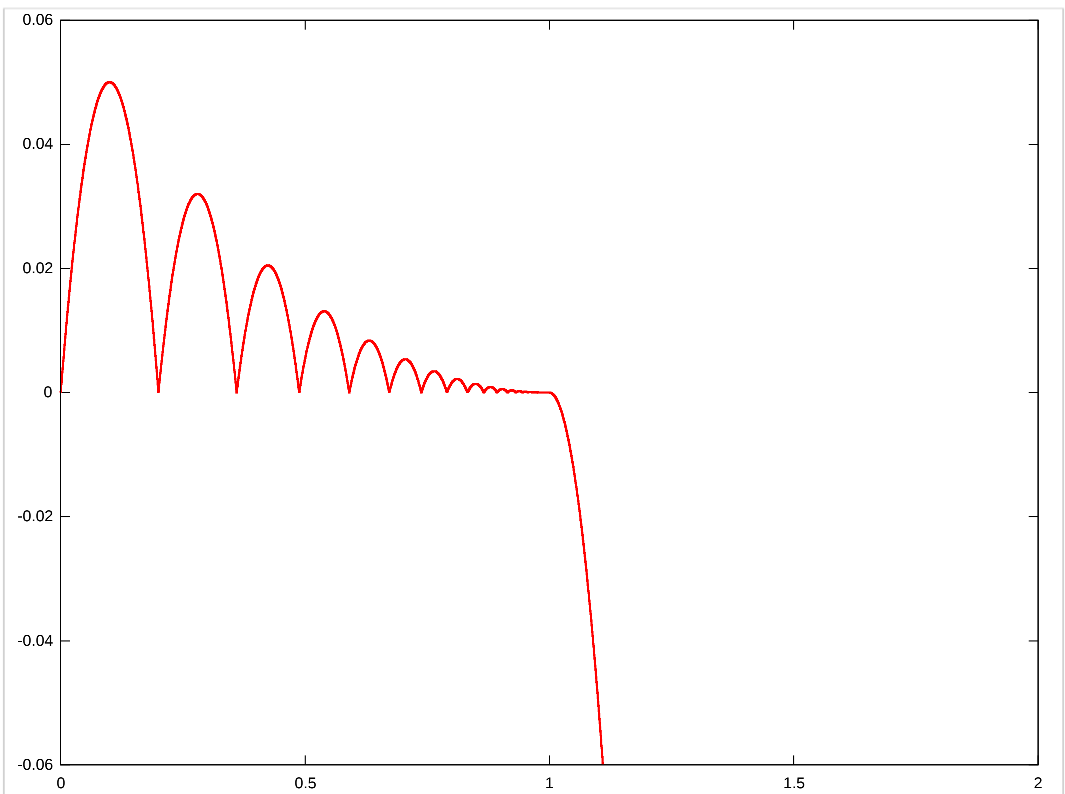
Appendix

```
model BouncingBall
   Real v, x;
   constant Real g = 10;
initial equation
   v = 1.0;
   x = 0.0;
equation
   der(v) = -g;
   der(x) = v;
   when x < 0 then
      reinit(v, -0.8 * pre(v));
      reinit(x, 0.0);
   end when;
end BouncingBall;
```

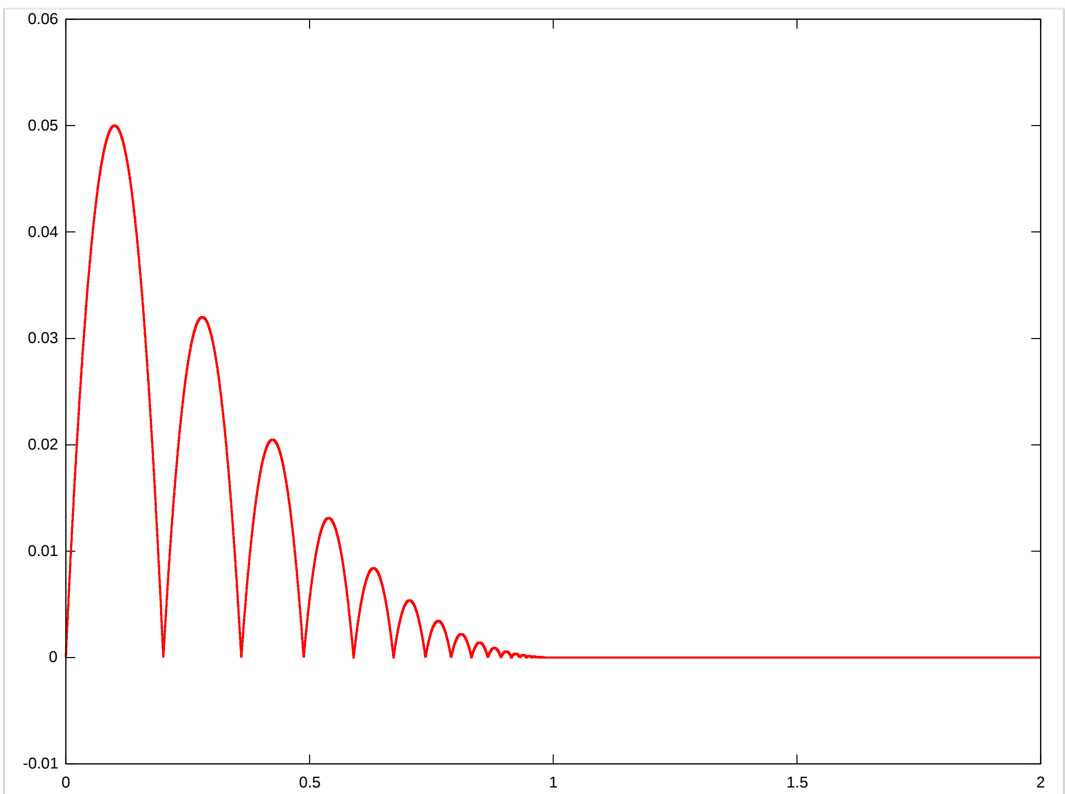
```
model BouncingBall
   Real v, x;
   constant Real g = 10;
initial equation
   v = 1.0;
   x = 0.0;
equation
   der(v) = -g;
   der(x) = v;
   when x < 0 then
      reinit(v, -0.8 * pre(v));
      reinit(x, 0.0);
   end when;
end BouncingBall;
```

```
model BouncingBall
   Real v, x;
   constant Real g = 10;
initial equation
   v = 1.0;
   x = 0.0;
equation
   der(v) = -g;
   der(x) = v;
   when x < 0 then
      reinit(v, -0.8 * pre(v));
      reinit(x, 0.0);
   end when;
end BouncingBall;
```

Which one is correct?

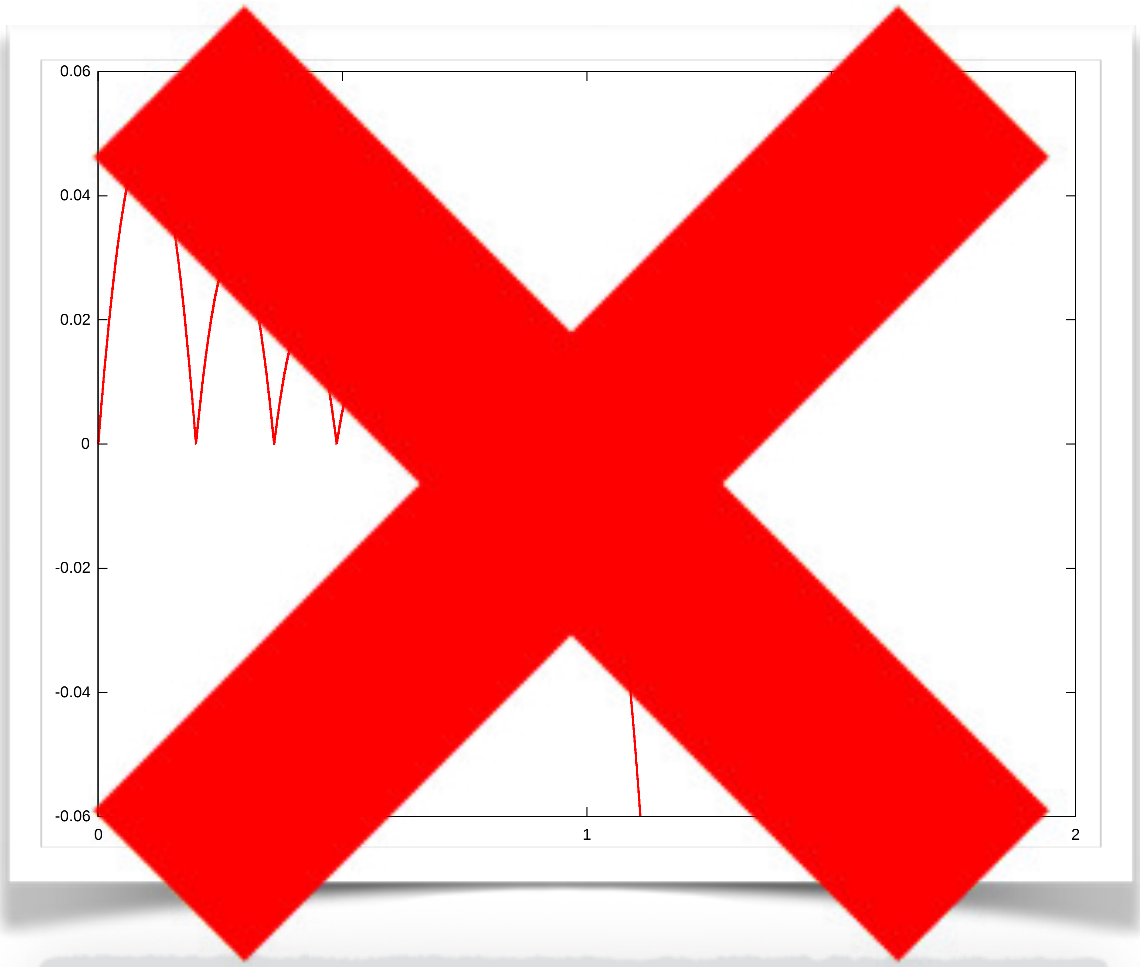


Results from simulator A



Results from simulator B

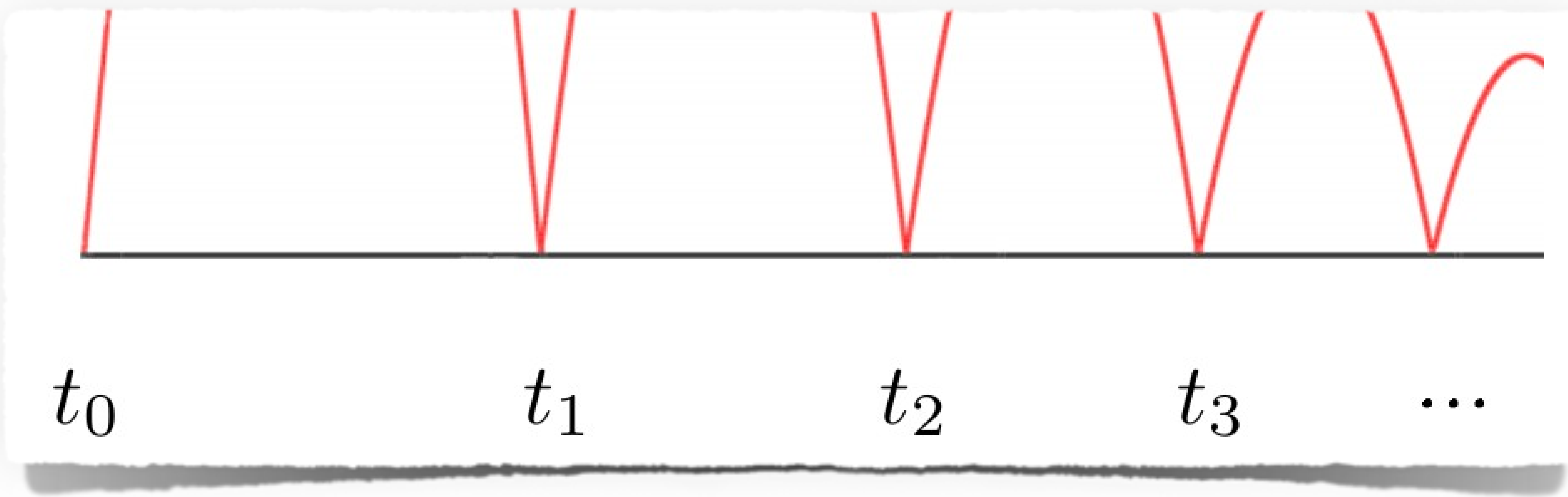
Which one is correct?



Results from simulator A

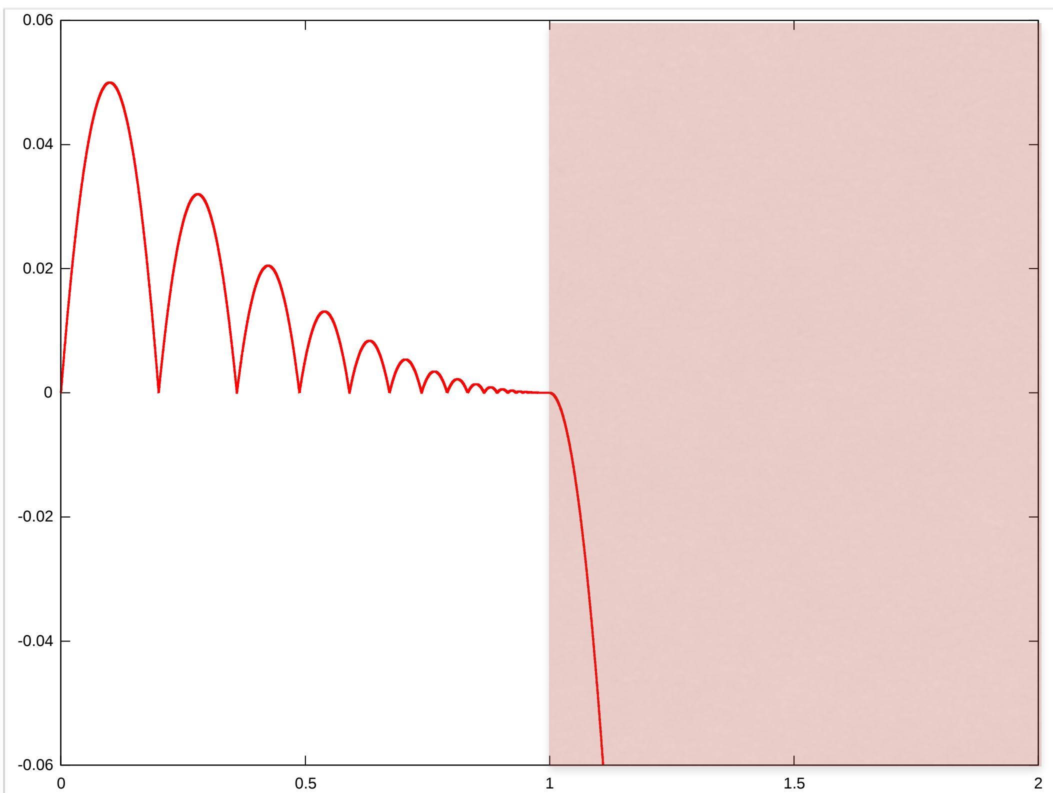
Results from simulator B

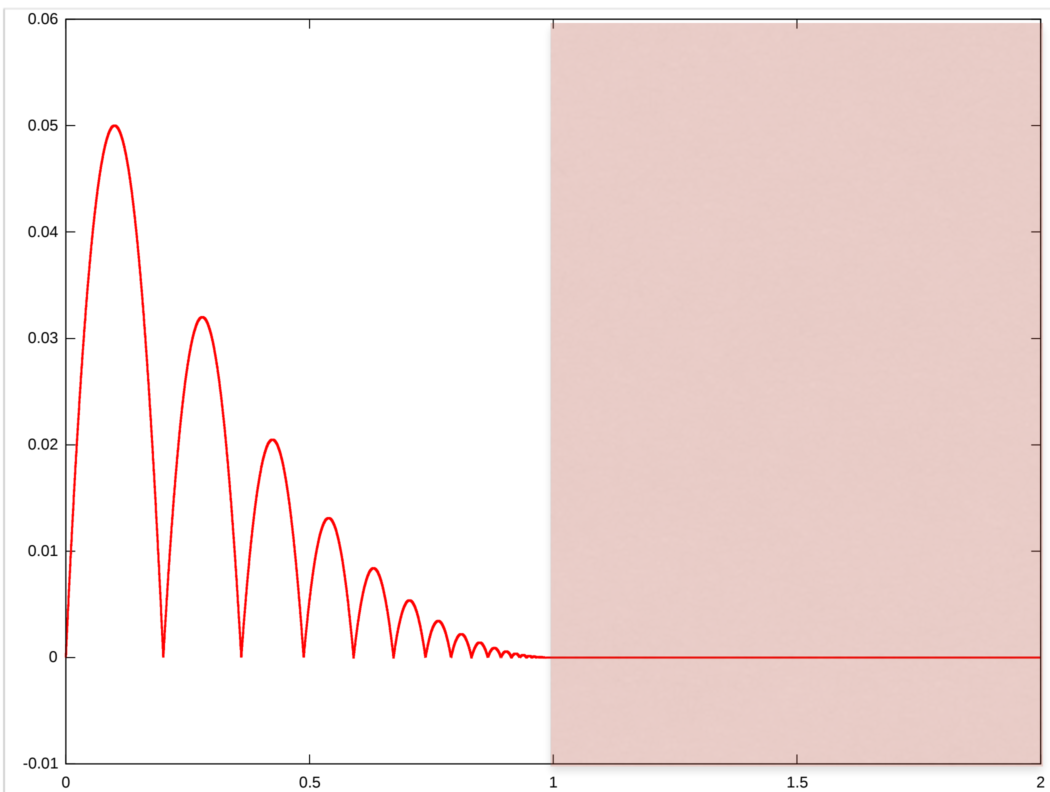
What's wrong?



$$\lim_{n\to\infty} t_n - t_0 = \frac{10v_0}{g} = 1$$

Zeno point

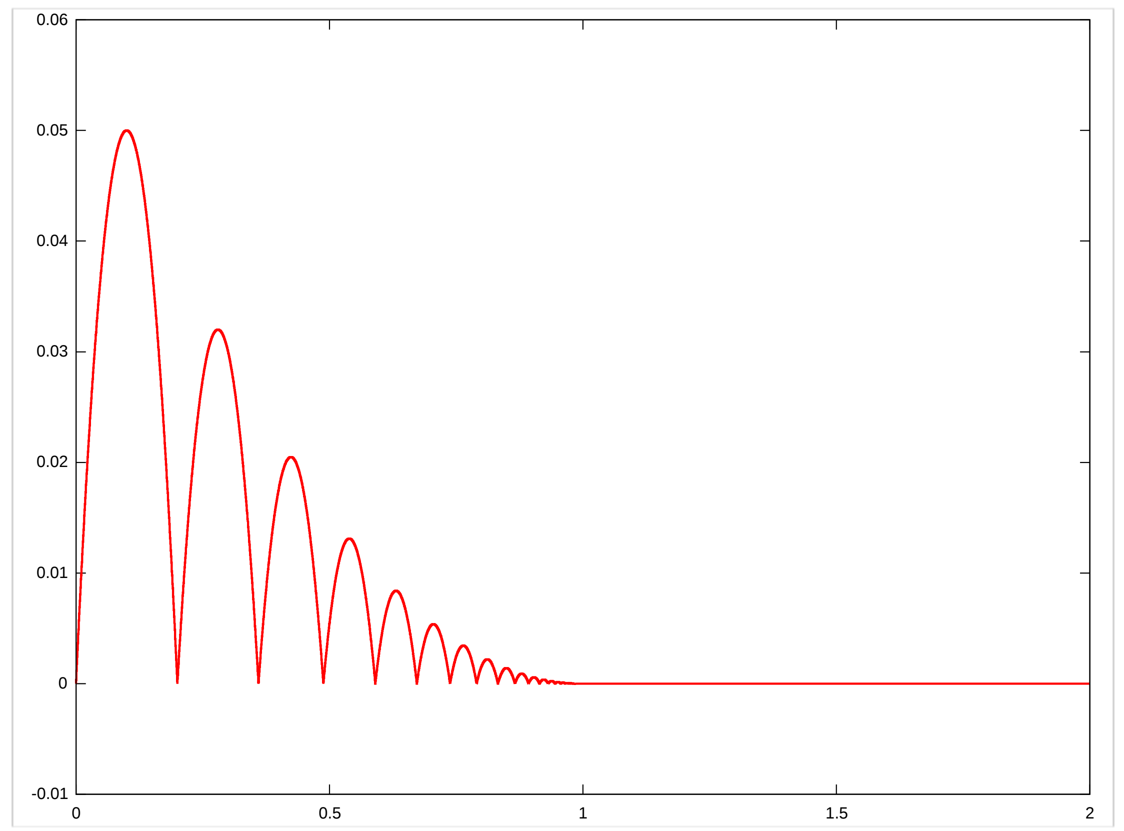




The model is undefined beyond the Zeno point!

Abstraction

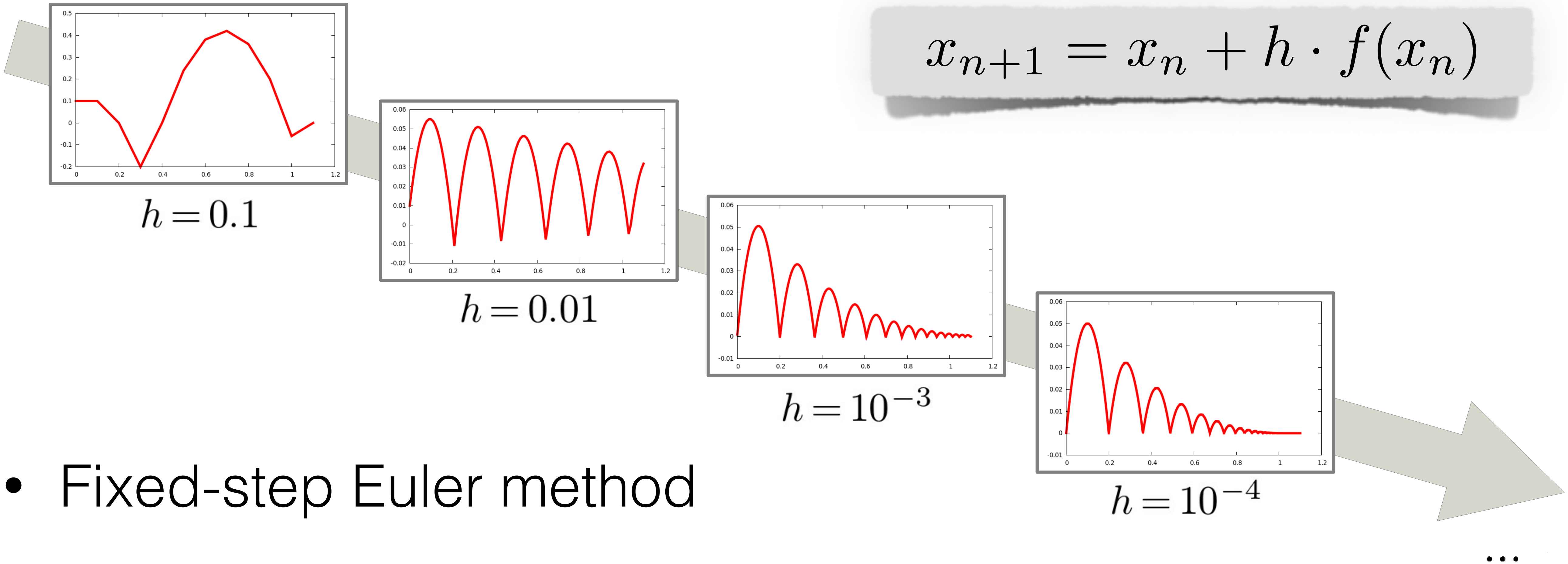
```
model BouncingBall
    Real v, x;
    constant Real g = 10;
initial equation
    v = 1.0;
    x = 0.0;
equation
    der(v) = -g;
    der(x) = v;
    when x < 0 then
        reinit(v, -0.8 * pre(v));
        reinit(x, 0.0);
    end when;
end BouncingBall;
```



This model is an **idealised** representation of the real-world behaviour of the ball.

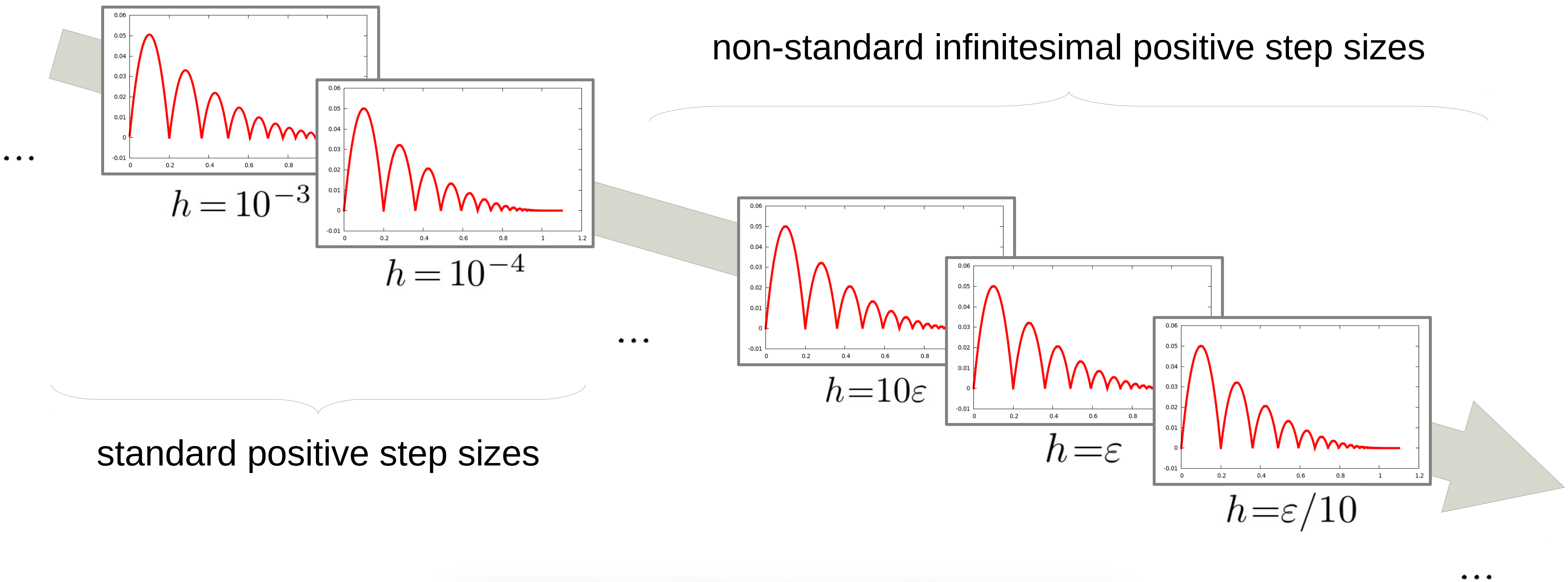
Approximation

$$x_{n+1} = x_n + h \cdot f(x_n)$$



- Fixed-step Euler method
- Approximates the desired model behaviour
  - Necessarily oversteps the Zeno point
- To fit all models, we need an **infinitesimal** step.

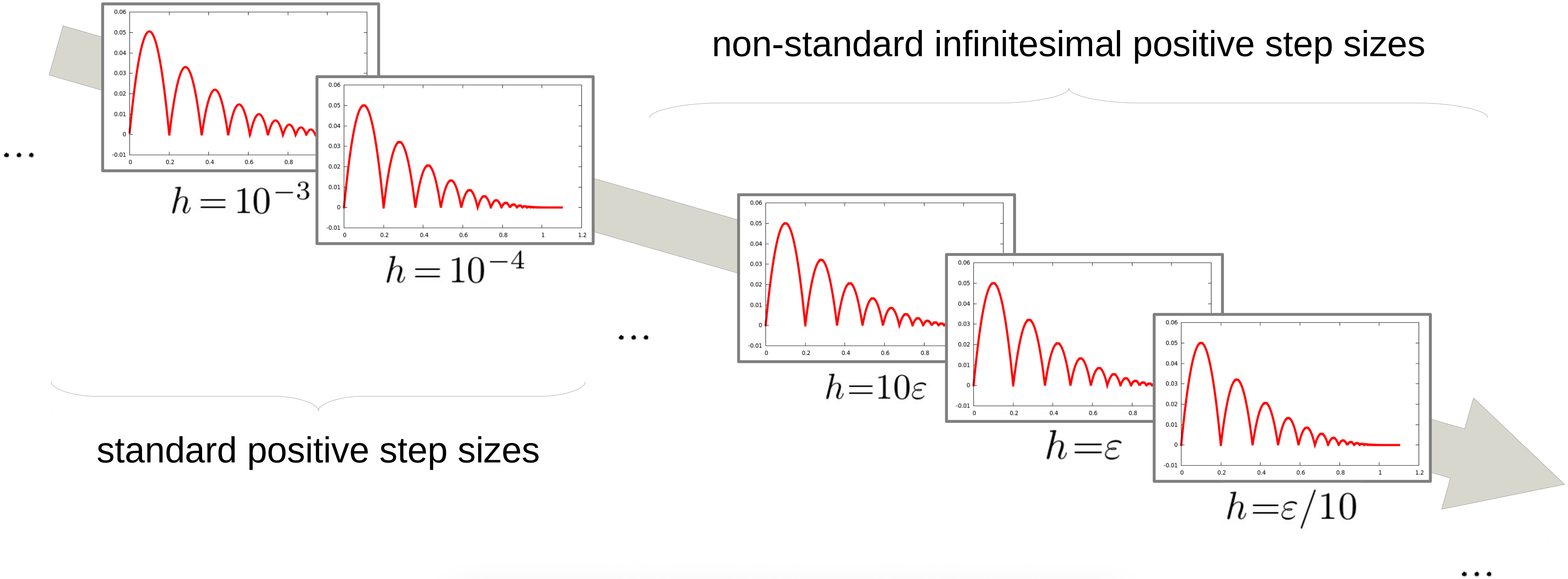
Non-standard semantics



$$ {}^*\mathbb{T} \stackrel{def}{=} \left\{ \varepsilon \cdot n \,\middle|\, n \in {}^*\mathbb{N}_0 \right\} $$

$$ \forall \varepsilon \approx 0,\ \forall x \in {}^*\mathbb{R},\ \exists n \in {}^*\mathbb{Z} :\ n\varepsilon < x \leq (n+1)\varepsilon $$

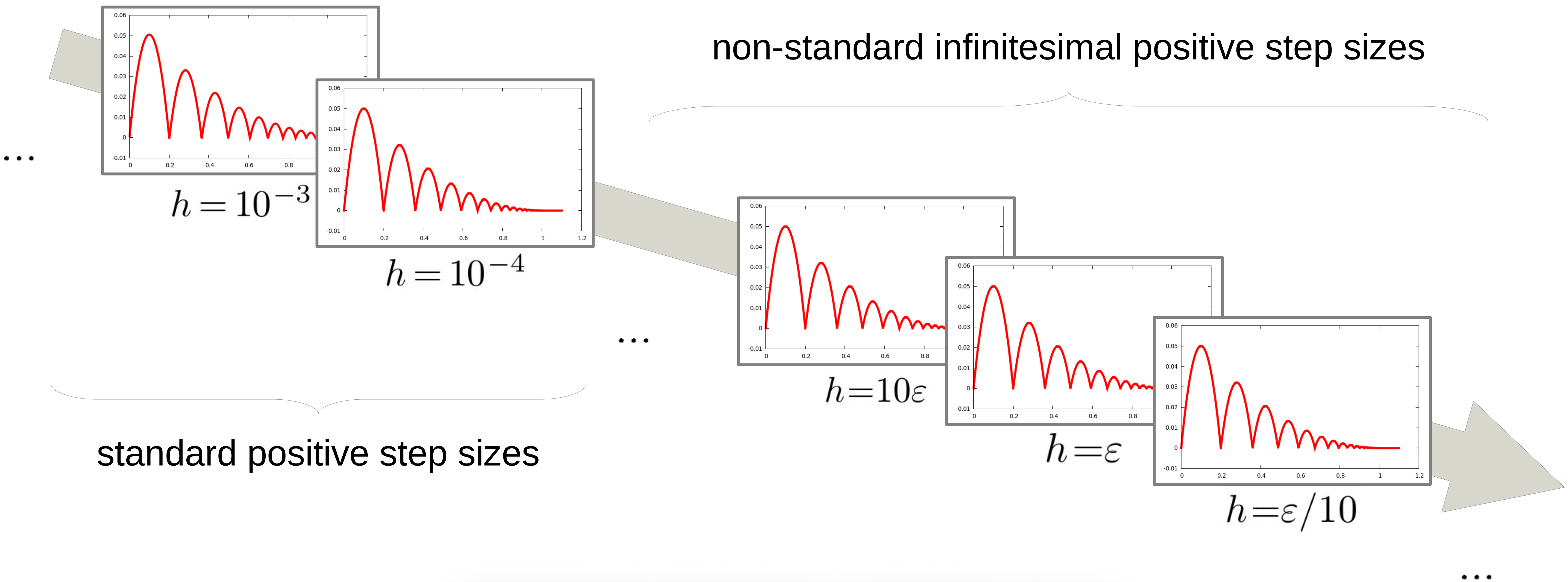
Non-standard semantics



$$^*\mathbb{T} \stackrel{def}{=} \left\{ \varepsilon \cdot n \,\middle|\, n \in {}^*\mathbb{N}_0 \right\}$$

$$\forall \varepsilon \approx 0,\ \forall x \in {}^*\mathbb{R},\ \exists n \in {}^*\mathbb{Z} :\ n\varepsilon < x \leq (n+1)\varepsilon$$

Non-standard semantics



$$^{*}\mathbb{T} \stackrel{def}{=} \left\{ \varepsilon \cdot n \,\middle|\, n \in {}^{*}\mathbb{N}_0 \right\}$$

$$\forall \varepsilon \approx 0,\ \forall x \in {}^{*}\mathbb{R},\ \exists n \in {}^{*}\mathbb{Z} :\ n\varepsilon < x \leq (n+1)\varepsilon$$