A Polynomial Template Abstract Domain based on Bernstein Polynomials

Pierre Roux [1]

April 8, 2013

[1]ONERA–DTIM, Toulouse

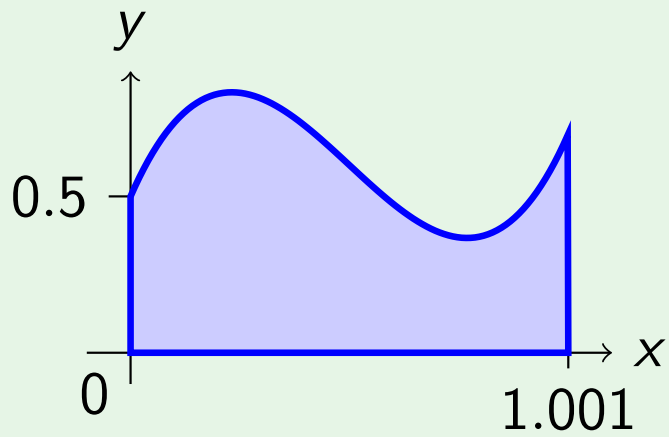
Example

Given program

x := 0; y := ?(0, 0.5);
while $x \leq 1$ **do**
    $y := y + 0.001 \times (18x^2 - 18x + 3)$;
    $x := x + 0.001$;
    if $y \leq 0$ **then** $y := 0$ **else** $y := y$ **fi od**

and templates $x, -x, y, -y$ and $y - 6x^3 + 9x^2 - 3.2x$,
we compute following loop invariant

$$\begin{aligned} x &\leq 1.001 \\ -x &\leq 0 \\ y &\leq 0.833 \\ -y &\leq 0 \\ y - 6x^3 + 9x^2 - 3.2x &\leq 0.5 \end{aligned}$$



Basic Idea

- Use **polynomial optimization** based on branch and bound algorithms using **Bernstein polynomials**
- as a back end for a **template domain** on **polynomial templates**.

Bernstein Polynomials

Definition (Bernstein Basis)

Any polynomial $p \in \mathbb{R}[\mathbf{x}]$ can be written

$$p(\mathbf{x}) = \sum_{\mathbf{0} \leq \mathbf{i} \leq \mathbf{d}} b_{p,\mathbf{i}} B_{\mathbf{d},\mathbf{i}}(\mathbf{x}) \quad \text{with} \quad B_{\mathbf{d},\mathbf{i}}(\mathbf{x}) = \prod_{j=1}^{n} \binom{d_j}{i_j} x_j^{i_j} (1-x_j)^{d_j - i_j}.$$

Bernstein Polynomials

Definition (Bernstein Basis)

Any polynomial $p \in \mathbb{R}[\mathbf{x}]$ can be written

$$p(\mathbf{x}) = \sum_{\mathbf{0} \leq \mathbf{i} \leq \mathbf{d}} b_{p,\mathbf{i}} B_{\mathbf{d},\mathbf{i}}(\mathbf{x}) \quad \text{with} \quad B_{\mathbf{d},\mathbf{i}}(\mathbf{x}) = \prod_{j=1}^{n} \binom{d_j}{i_j} x_j^{i_j} (1-x_j)^{d_j - i_j}.$$

Property

For all $\mathbf{x} \in [\mathbf{0}, \mathbf{1}]$,

$$\min \{ b_{p,\mathbf{i}} \mid \mathbf{0} \leq \mathbf{i} \leq \mathbf{d} \} \leq p(\mathbf{x}) \leq \max \{ b_{p,\mathbf{i}} \mid \mathbf{0} \leq \mathbf{i} \leq \mathbf{d} \}.$$

Bernstein Polynomials

Definition (Bernstein Basis)

Any polynomial $p \in \mathbb{R}[\mathbf{x}]$ can be written

$$p(\mathbf{x}) = \sum_{\mathbf{0} \leq \mathbf{i} \leq \mathbf{d}} b_{p,\mathbf{i}} B_{\mathbf{d},\mathbf{i}}(\mathbf{x}) \quad \text{with} \quad B_{\mathbf{d},\mathbf{i}}(\mathbf{x}) = \prod_{j=1}^{n} \binom{d_j}{i_j} x_j^{i_j} (1-x_j)^{d_j - i_j}.$$

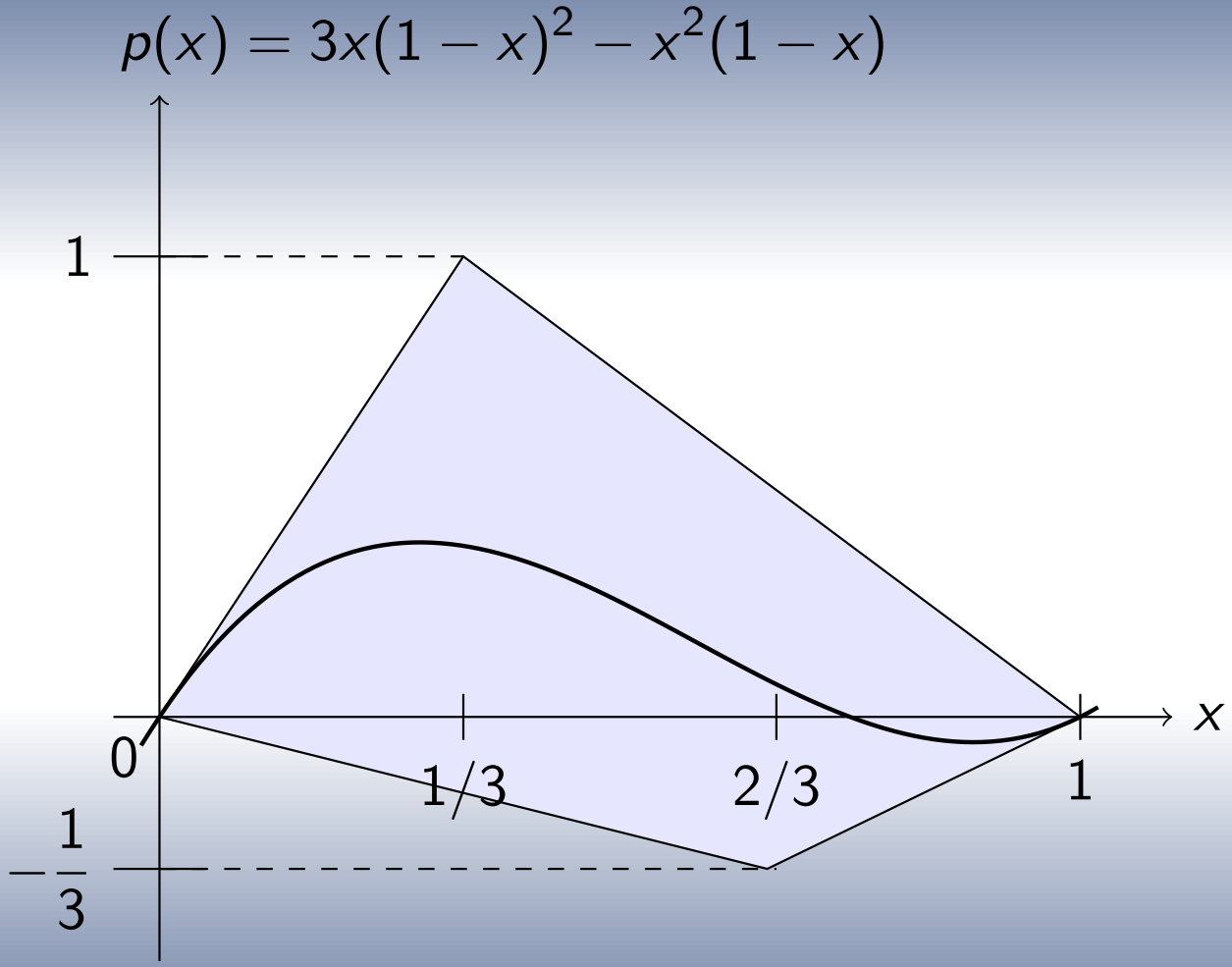
Property

For all $\mathbf{x} \in [\mathbf{0}, \mathbf{1}]$,

$$\min \{b_{p,\mathbf{i}} \mid \mathbf{0} \leq \mathbf{i} \leq \mathbf{d}\} \leq p(\mathbf{x}) \leq \max \{b_{p,\mathbf{i}} \mid \mathbf{0} \leq \mathbf{i} \leq \mathbf{d}\}.$$

Moreover, $p(\mathbf{i}) = b_{p,\mathbf{i}}$ for all $\mathbf{i} \in \mathcal{C}_{\mathbf{d}}$
where $\mathcal{C}_{\mathbf{d}} = \{\mathbf{i} \in \mathbb{N}^n \mid \forall j, 0 \leq j \leq n \Rightarrow (i_j = 0 \vee i_j = d_j)\}$.

Bernstein Polynomials, Illustration



Optimization Problem

Definition ($\mathrm{Opt}(p; q_1, \ldots, q_k)(b_1, \ldots, b_k)$)

We want to compute an overapproximation of

$$\max\{p(\mathbf{x}) \mid q_1(\mathbf{x}) \leq b_1 \wedge \ldots \wedge q_k(\mathbf{x}) \leq b_k\}$$

where $\{ q_1, \ldots, q_k \}$ includes polynomials x_i and $-x_i$ for all variables x_i.

Optimization Problem

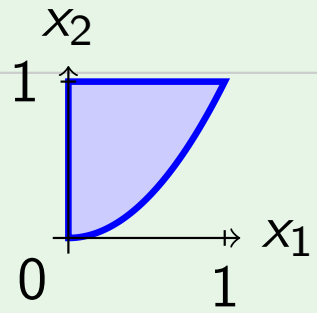
Definition ($\mathrm{Opt}(p; q_1, \ldots, q_k)(b_1, \ldots, b_k)$)

We want to compute an overapproximation of

$$\max\{p(\mathbf{x}) \mid q_1(\mathbf{x}) \leq b_1 \wedge \ldots \wedge q_k(\mathbf{x}) \leq b_k\}$$

where $\{ q_1, \ldots, q_k \}$ includes polynomials x_i and $-x_i$ for all variables x_i.

Example



- $\mathrm{Opt}\left(x_1 + x_2; x_1, -x_1, x_2, -x_2, x_1^2 - x_2\right)(1, 0, 1, 0, 0) = 2$
- $\mathrm{Opt}\left(x_1 + x_2; x_1, -x_1, x_2, -x_2, x_1^2 - x_2\right)(1, 0, 1, 0, -1.1) = -\infty.$

Branch and Bound Algorithm

A polynomial p of degree d on Bernstein form cen be split in $p_{left}(x) = p\left(\frac{x}{2}\right)$ and $p_{right}(x) = p\left(\frac{x+1}{2}\right)$ (by de Casteljau's algorithm in $\Theta(d^2)$ arithmetic operations).

Branch and Bound Algorithm

A polynomial p of degree d on Bernstein form cen be split in $p_{left}(x) = p\left(\frac{x}{2}\right)$ and $p_{right}(x) = p\left(\frac{x+1}{2}\right)$ (by de Casteljau's algorithm in $\Theta(d^2)$ arithmetic operations).

Hence a branch and bound algorithm

- If $\min\{b_{q_i,\mathbf{j}} \mid \mathbf{0} \leq \mathbf{j} \leq \mathbf{d}\} > b_i$ for some q_i, constraint q_i is unsatisfiable on unit box, return $-\infty$.
- If $\max\{b_{p,\mathbf{i}} \mid \mathbf{0} \leq \mathbf{i} \leq \mathbf{d}\} - \max\left\{b_{p,\mathbf{i}} \;\middle|\; \mathbf{i} \in \mathcal{C}_{\mathbf{d}} \wedge \forall j, b_{q_j,\mathbf{i}} \leq b_j\right\} \leq \epsilon$, return $\max\{b_{p,\mathbf{i}} \mid \mathbf{0} \leq \mathbf{i} \leq \mathbf{d}\}$.
- Otherwise, split p in p_{left} and p_{right} and treat them recursively.

Relaxation

An alternative algorithm using a relaxation allows to
get rid of polynomial constraints by putting them in the objective.

- Can induce an overapproximation.
- Sometime more efficient.

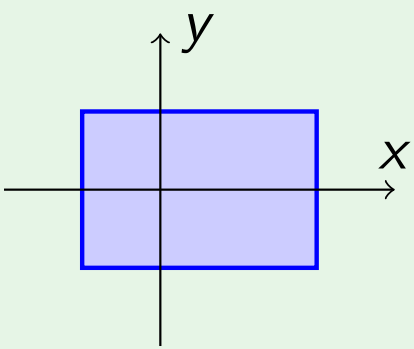
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

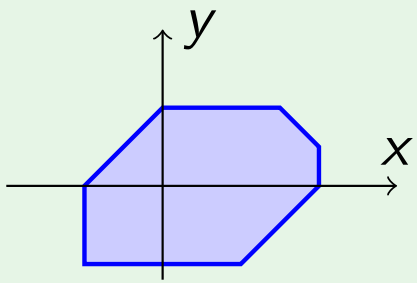
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

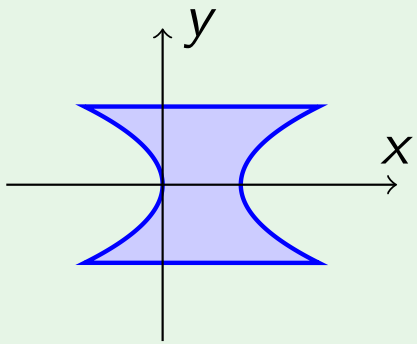
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

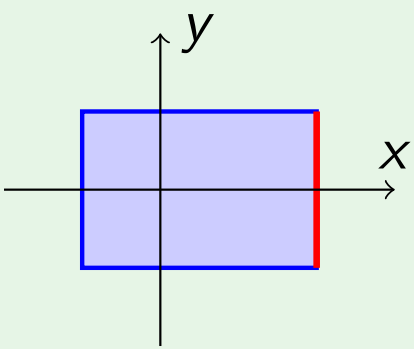
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

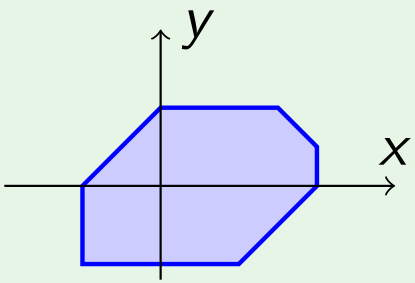
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

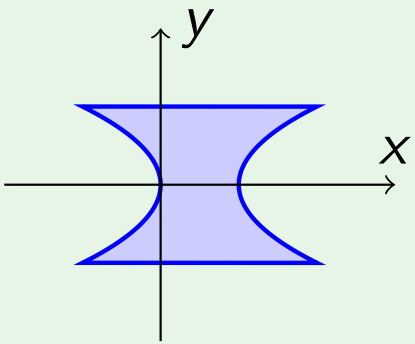
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

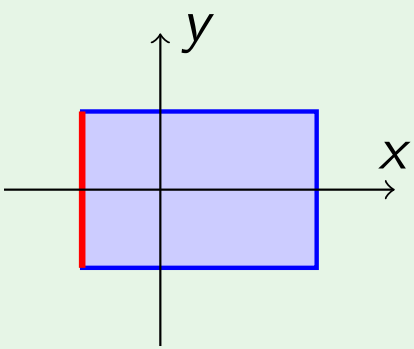
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

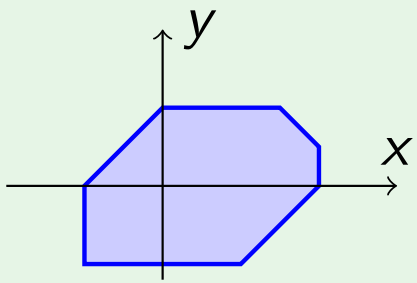
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

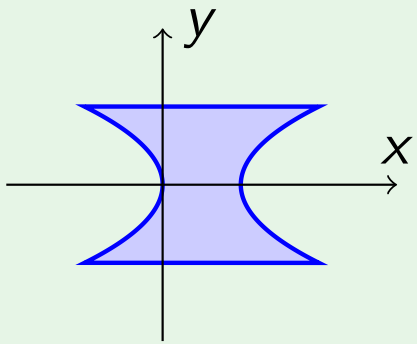
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

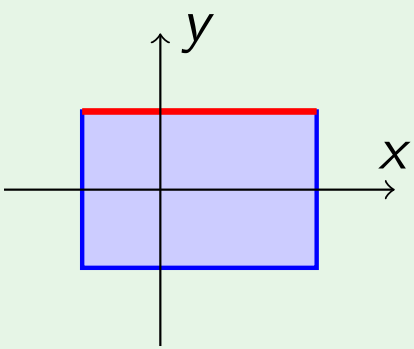
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

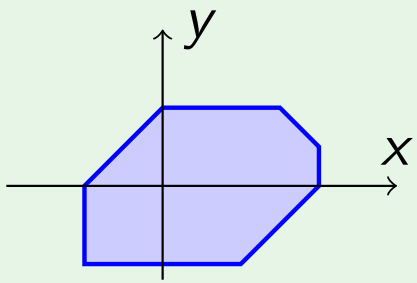
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

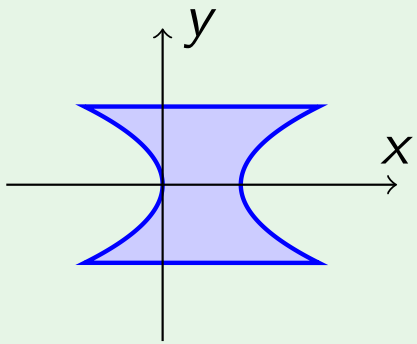
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

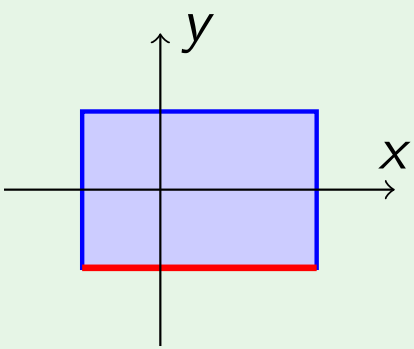
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

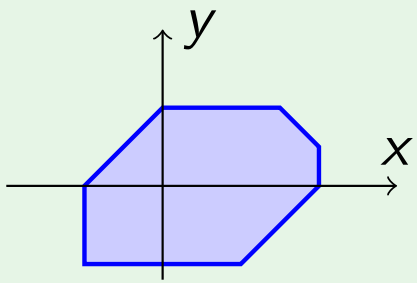
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

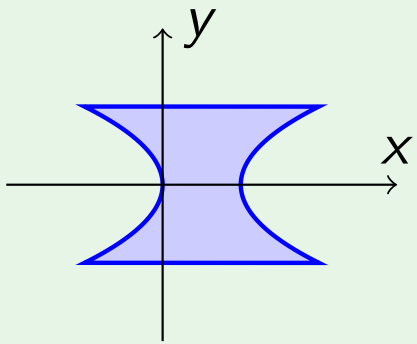
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

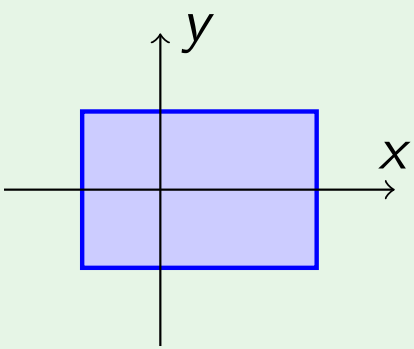
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

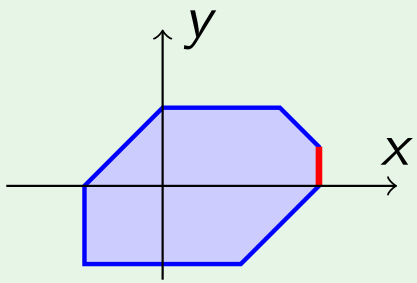
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

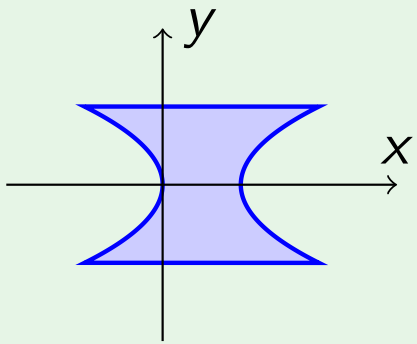
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

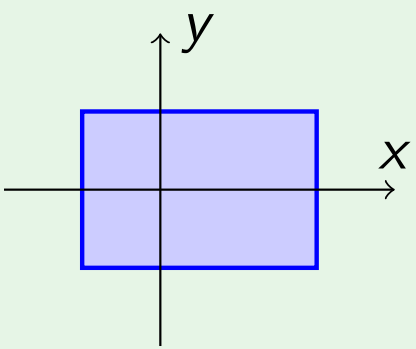
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

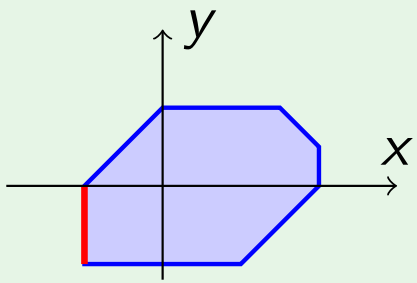
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

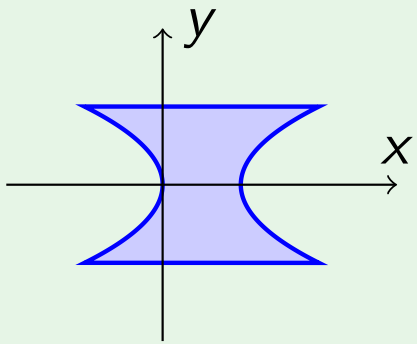
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

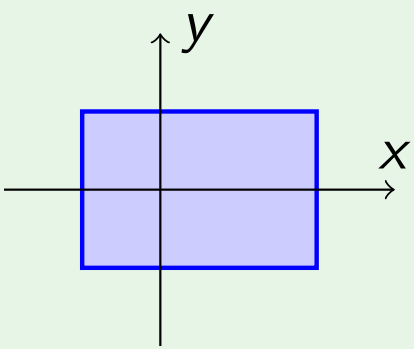
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

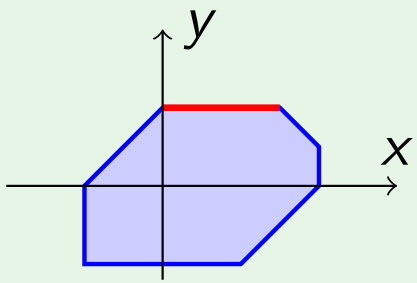
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

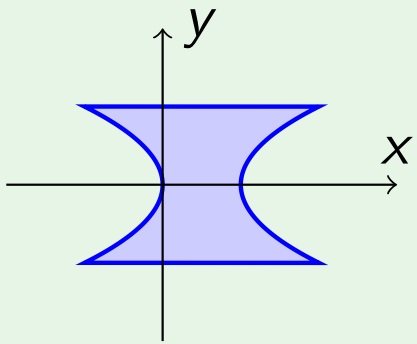
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

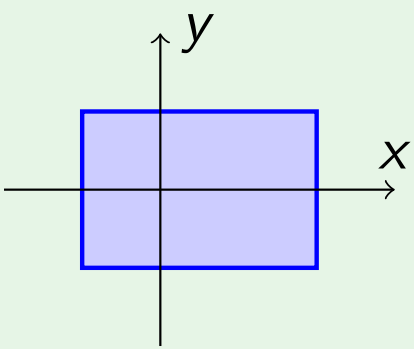
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

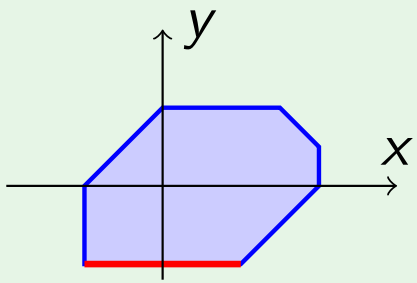
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

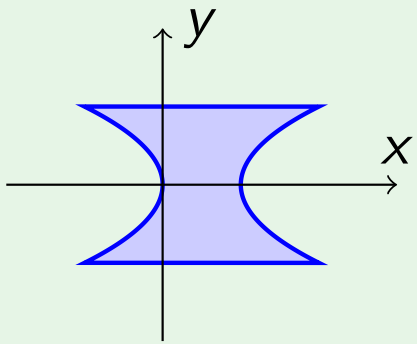
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

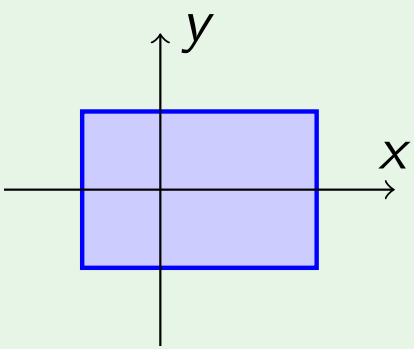
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

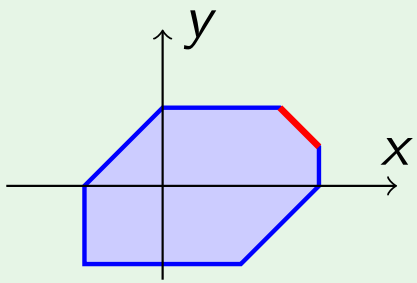
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

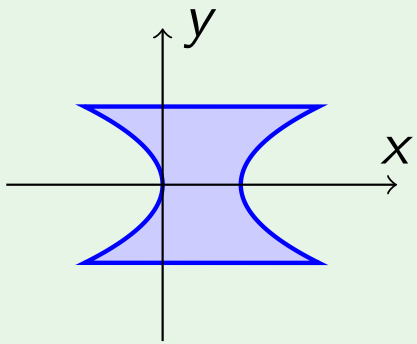
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

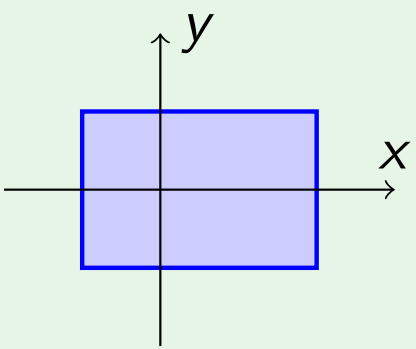
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

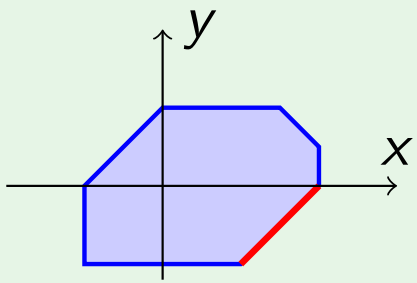
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

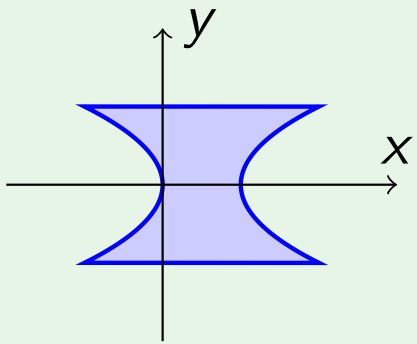
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

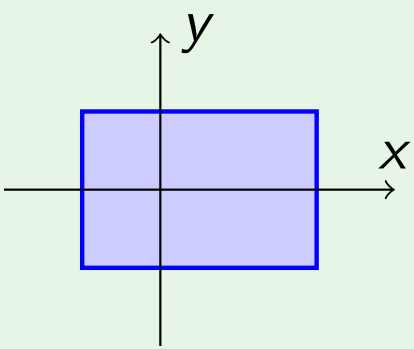
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

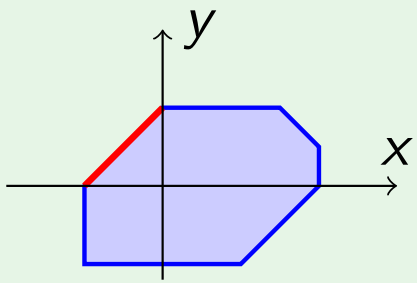
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

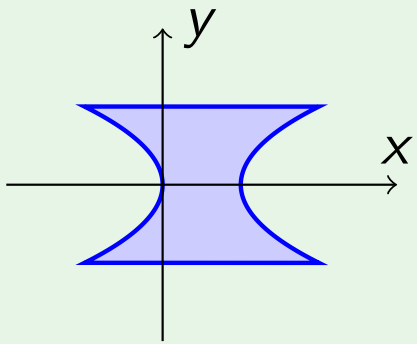
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

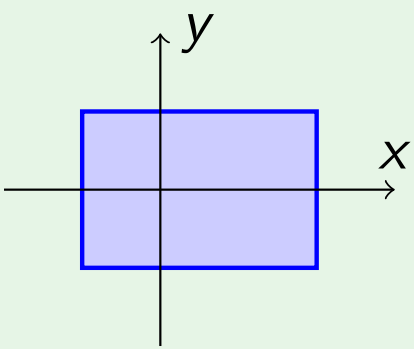
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

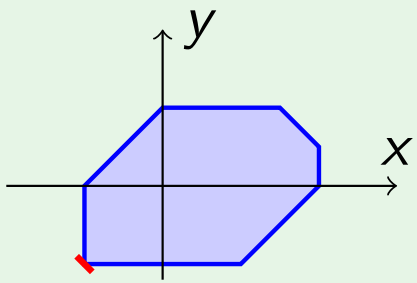
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

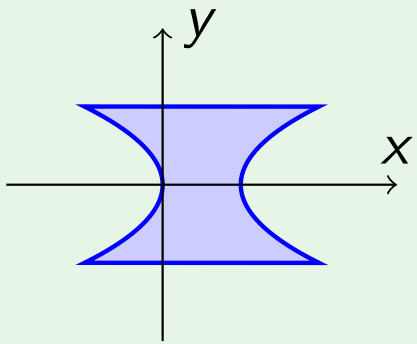
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

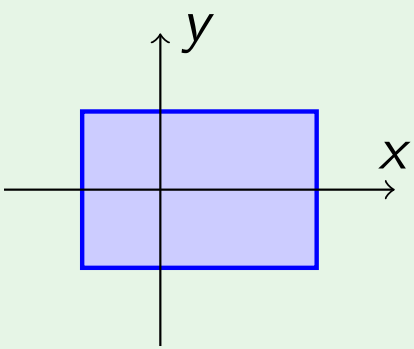
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

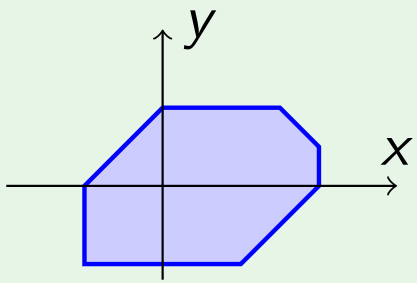
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

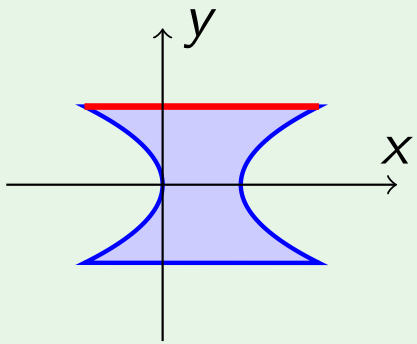
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

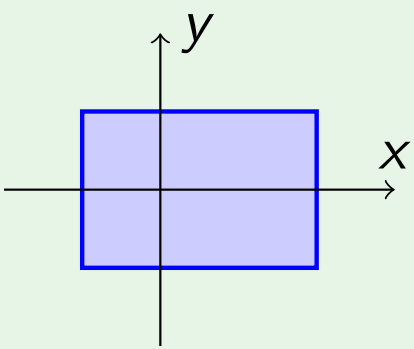
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

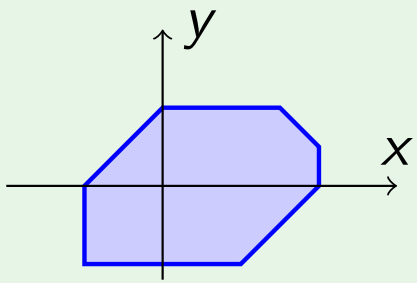
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

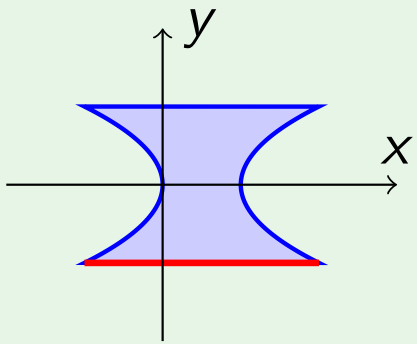
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

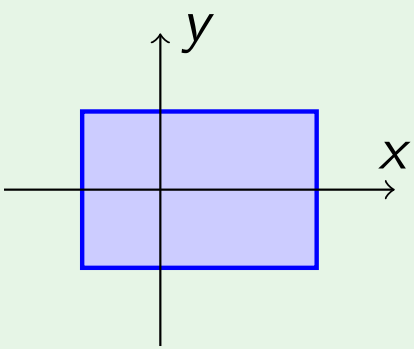
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

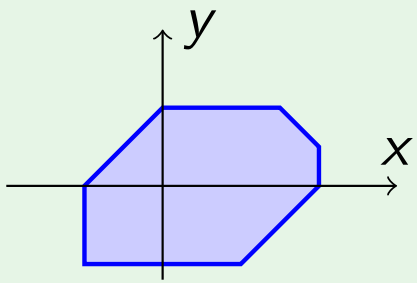
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

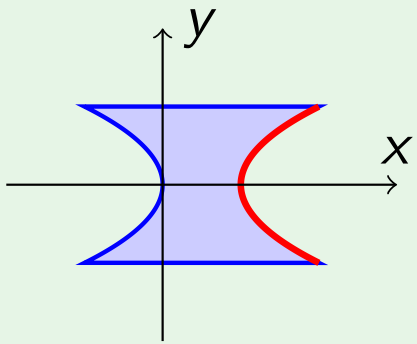
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$



quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

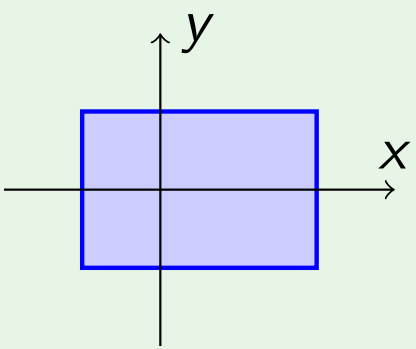
Template Domains

Definition (Template Domain)

Given a set of expressions $\mathcal{T} = \{ t_1, \ldots, t_n \}$, abstract values are tuples $(b_1, \ldots, b_n) \in \overline{\mathbb{R}}^n = (\mathbb{R} \cup \{ \pm\infty \})^n$, representing $\gamma_{\mathcal{T}}(b_1, \ldots, b_n) = \{\rho \in (\mathbb{V} \to \mathbb{R}) \mid t_1(\rho) \leq b_1, \ldots, t_n(\rho) \leq b_n\}$.

Example

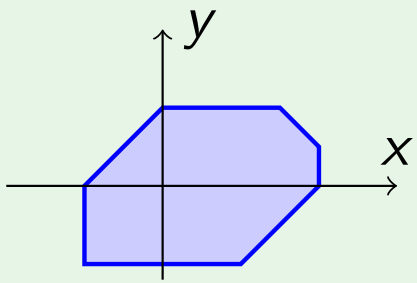
$(2, 1, 1, 1)$



intervals

$(\mathcal{T} = \{ x, -x, y, -y \})$

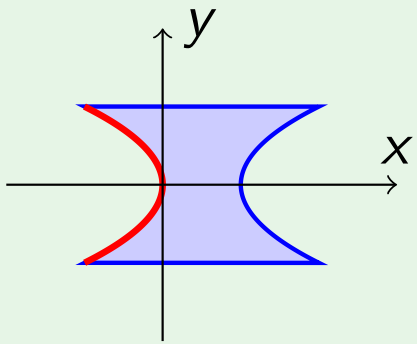
$(2, 1, 1, 1, 2.5, 2, 1, 2)$



octagons

$$(\mathcal{T} = \left\{ \begin{array}{c} x, -x, y, -y, \\ x+y, x-y, \\ -x+y, -x-y \end{array} \right\})$$

$(1, 1, 1, 1)$

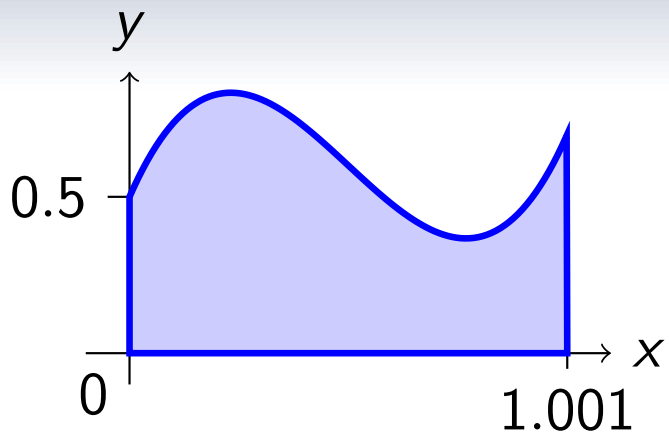


quadratic

$(\mathcal{T} = \{ y, -y, x - y^2, -y^2 - x \})$

Template Domains, Example

$$
\begin{array}{rcl}
x & \leq & 1.001 \\
-x & \leq & 0 \\
y & \leq & 0.833 \\
-y & \leq & 0 \\
y - 6x^3 + 9x^2 - 3.2x & \leq & 0.5
\end{array}
$$



Abstract Operator for Guards

Definition

We define the abstract semantic of a guard $r(\mathbf{x}) \leq 0$ on an abstract value $\mathbf{b}$ as

$$[\![r(\mathbf{x}) \leq 0]\!]^\sharp (\mathbf{b}) = \mathbf{b'}$$

where $b'_i = \mathrm{Opt}(p_i; p_1, \ldots, p_k, r)\,(b_1, \ldots, b_k, 0)$.

Example

Using templates $\mathcal{T} = \{ x, -x, y, -y, y - 6x^3 + 9x^2 - 3.2x \}$,
$[\![x - 1 \leq 0]\!]^\sharp (10, 0, 10, 0, 0.5) = (1, 0, 0.833, 0, 0.5)$.

Abstract Operator for Assignments

Definition

We define the abstract semantic of an assignment $x_i := r$ on an abstract value $\mathbf{b}$ as

$$[\![x_i := r]\!]^\sharp(\mathbf{b}) = \mathbf{b}'$$

where $b'_j = \mathrm{Opt}(p_j[x_i \leftarrow r(\mathbf{x})]; p_1, \ldots, p_k)(\mathbf{b})$.

Example

Still with $\mathcal{T} = \{ x, -x, y, -y, y - 6x^3 + 9x^2 - 3.2x \}$,
$[\![y := 0]\!]^\sharp(1.001, -0.001, 0, 0.002, 0.133)$
$= (1.001, -0.001, 0, 0, 0.133)$.

Abstract Operator for Random Assignments

Definition

We define the semantic of a random assignment $x_i := ?(r_1, r_2)$ on an abstract value $\mathbf{b}$ with $r_1, r_2 \in \mathbb{R}$ as

$$[\![x_i := ?(r_1, r_2)]\!]^\sharp(\mathbf{b}) = \rho(\mathbf{b'})$$

where

$$b'_i = \begin{cases} r2 & \text{if } p_i = x_i \\ -r1 & \text{if } p_i = -x_i \\ +\infty & \text{otherwise, if } x_i \text{ appears in } p_i \\ b_i & \text{otherwise.} \end{cases}$$

where $\rho : \mathcal{T}_P \to \mathcal{T}_P$ is defined as $\rho(\mathbf{b}) = \mathbf{b'}$ with $b'_i = \mathrm{Opt}(p_i; p_1, \ldots, p_k)(\mathbf{b})$.

Example

$[\![y := ?(0, 0.5)]\!]^\sharp(0, 0, +\infty, +\infty, +\infty) = (0, 0, 0.5, 0, 0.5)$.

Widening

Assuming a widening on lattice $\overline{\mathbb{R}}$
its pointwise extension is a widening on our domain.

Widening

Assuming a widening on lattice $\overline{\mathbb{R}}$
its pointwise extension is a widening on our domain.

In practice, jumping directly to $+\infty$
on a bound b_i for templates x or $-x$ defining the considered box
could completely spoil results ($+\infty$ propagates to other bounds).

Widening

Assuming a widening on lattice $\overline{\mathbb{R}}$
its pointwise extension is a widening on our domain.

In practice, jumping directly to $+\infty$
on a bound b_i for templates x or $-x$ defining the considered box
could completely spoil results ($+\infty$ propagates to other bounds).

A widening such as a widening with threshold
should be used to avoid this.

Implementation Considerations

- Choice of parameter ϵ (accuracy of optimization algorithm) plays a key role in the precision/cost trade off.

Implementation Considerations

- Choice of parameter ϵ (accuracy of optimization algorithm) plays a key role in the precision/cost trade off.
- Optimization algorithms make intensive arithmetic computations,

Implementation Considerations

- Choice of parameter ϵ (accuracy of optimization algorithm) plays a key role in the precision/cost trade off.
- Optimization algorithms make intensive arithmetic computations, just using floating point computations would be unsound

Implementation Considerations

- Choice of parameter ϵ (accuracy of optimization algorithm) plays a key role in the precision/cost trade off.
- Optimization algorithms make intensive arithmetic computations, just using floating point computations would be unsound and rationals are expensive.

Implementation Considerations

- Choice of parameter ϵ (accuracy of optimization algorithm) plays a key role in the precision/cost trade off.
- Optimization algorithms make intensive arithmetic computations, just using floating point computations would be unsound and rationals are expensive.
- Floating point interval arithmetic is a good solution (sound, precise and only about two times slower than (unsound) pure floating points in practice).

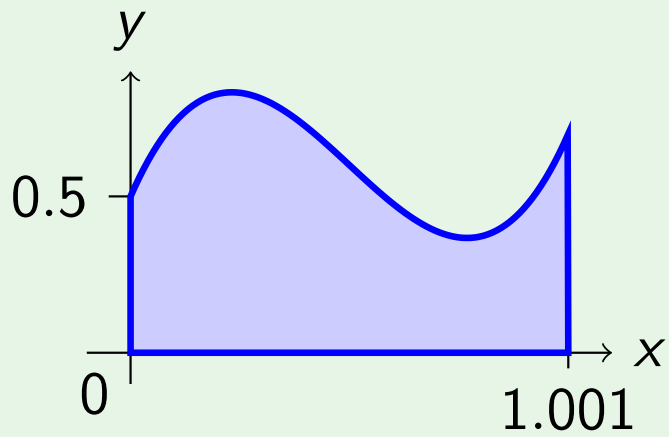
Example

Given program

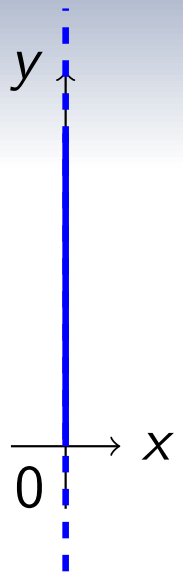
x := 0; y := ?(0, 0.5);
while $x \leq 1$ **do**
    $y := y + 0.001 \times (18x^2 - 18x + 3)$;
    $x := x + 0.001$;
    if $y \leq 0$ **then** $y := 0$ **else** $y := y$ **fi od**

and templates $x, -x, y, -y$ and $y - 6x^3 + 9x^2 - 3.2x$,
we compute following loop invariant

$$\begin{aligned} x &\leq 1.001 \\ -x &\leq 0 \\ y &\leq 0.833 \\ -y &\leq 0 \\ y - 6x^3 + 9x^2 - 3.2x &\leq 0.5 \end{aligned}$$

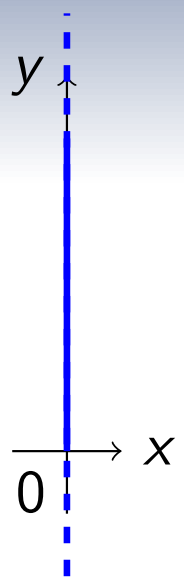


Example

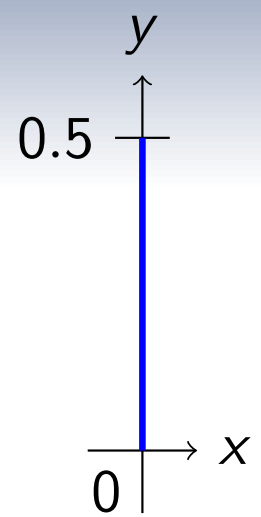


$(a) = \top$ $(b) = [\![x := 0]\!]^\sharp(a) = (0, 0, +\infty, +\infty, +\infty)$

Example

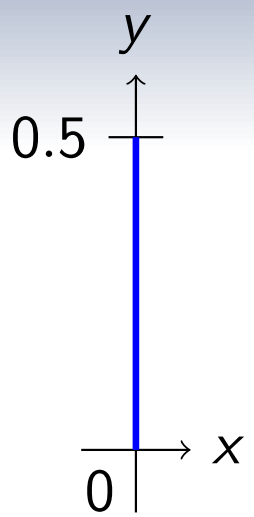


$(\mathrm{b}) = (0, 0, +\infty, +\infty, +\infty)$

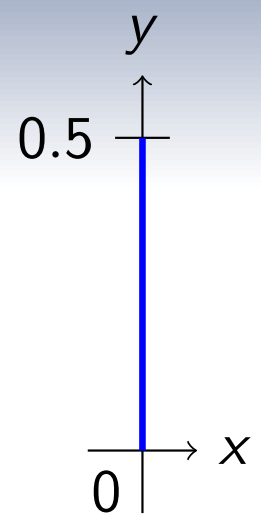


$(\mathrm{c}) = [\![y := ?(0, 0.5)]\!]^\sharp(\mathrm{b}) =$
$(0, 0, 0.5, 0, 0.5)$

Example

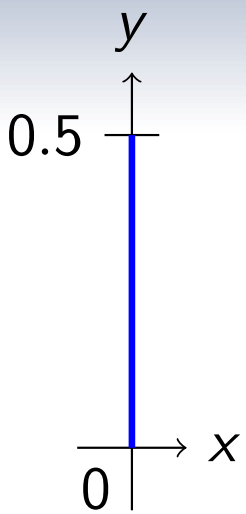


$(c) = (0, 0, 0.5, 0, 0.5)$

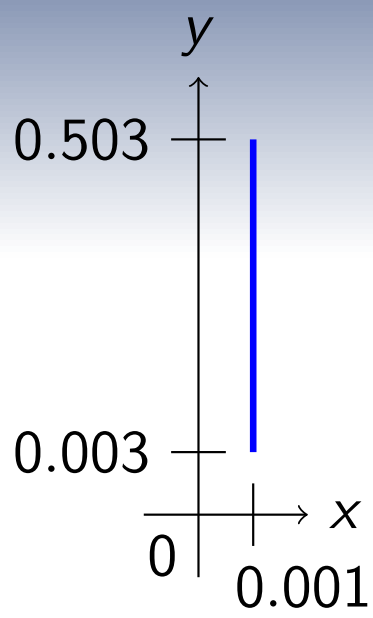


$(d) = [\![x - 1 \leq 0]\!]^\sharp(c) = (0, 0, 0.5, 0, 0.5)$

Example

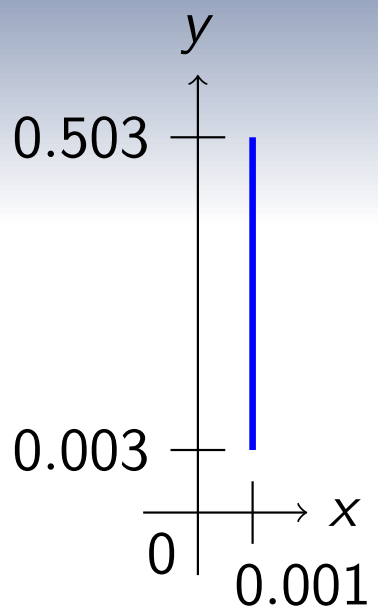


$(\mathrm{d}) = (0, 0, 0.5, 0, 0.5)$



$(\mathrm{e}) = [\![y := y + 0.001(18x^2 - 18x + 3); x := x + 0.001]\!]^\sharp(\mathrm{d}) = (0.001, -0.001, 0.503, -0.003, 0.5)$

Example



$$(\mathrm{e}) = (0.001, -0.001, 0.503, -0.003, 0.5)$$

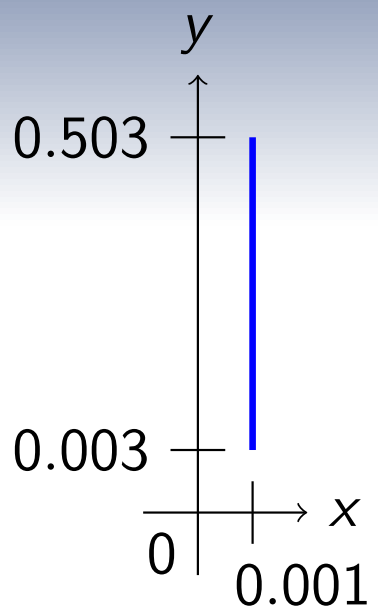
$$(\mathrm{f}) = [\![y \leq 0]\!]^\sharp(\mathrm{e}) = \bot$$

Example

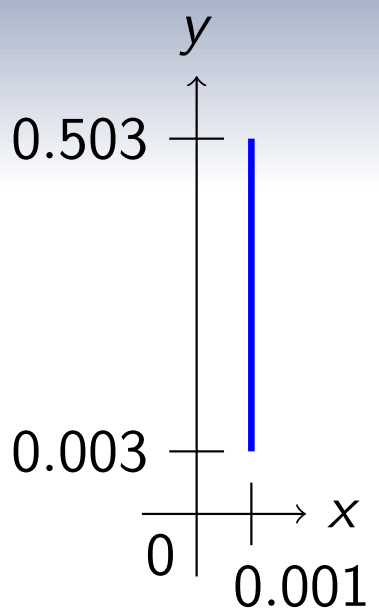
$(\mathrm{f}) = \bot$

$(\mathrm{g}) = [\![y := 0]\!]^\sharp(\mathrm{f}) = \bot$

Example

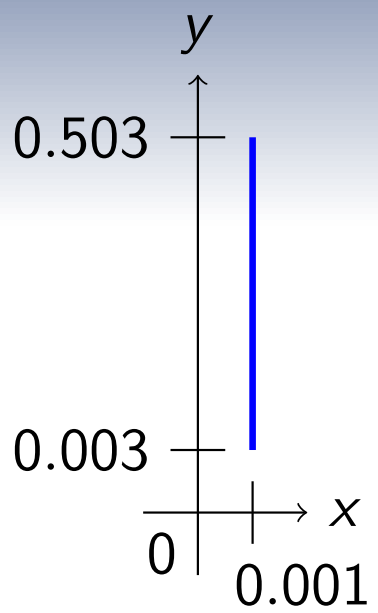


$$(\mathrm{e}) =$$
$$(0.001, -0.001, 0.503, -0.003, 0.5)$$

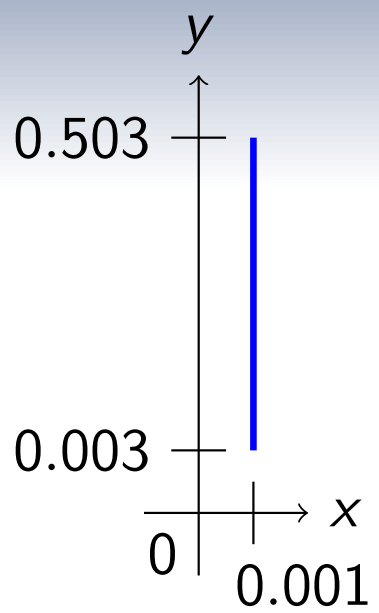


$$(\mathrm{h}) = [\![y \geq 0]\!]^\sharp(\mathrm{e}) = (\mathrm{e})$$

Example

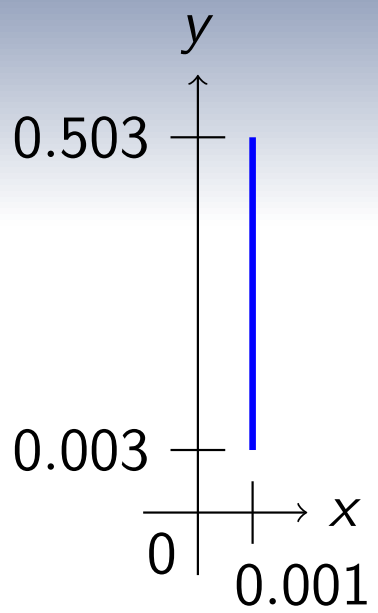


$$(\mathrm{h}) =$$
$$(0.001, -0.001, 0.503, -0.003, 0.5)$$



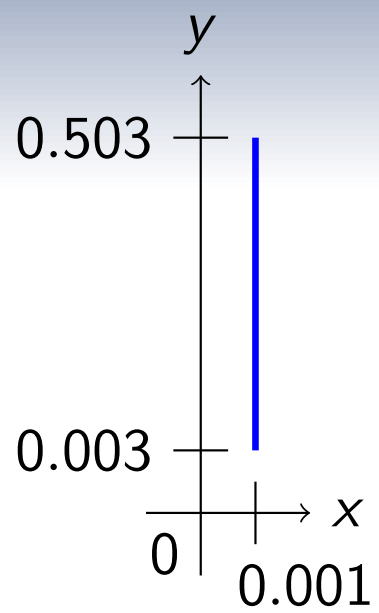
$$(\mathrm{i}) = [\![y := y]\!]^\sharp(\mathrm{h}) = (\mathrm{h})$$

Example



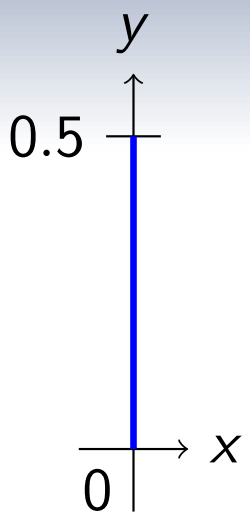
$(\mathrm{g}) = \bot \qquad (\mathrm{i}) =$

$(0.001, -0.001, 0.503, -0.003, 0.5)$

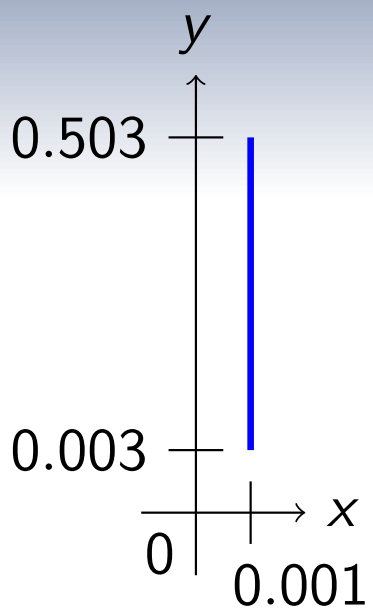


$(\mathrm{j}) = (\mathrm{g}) \sqcup^{\sharp} (\mathrm{i}) = (\mathrm{i})$

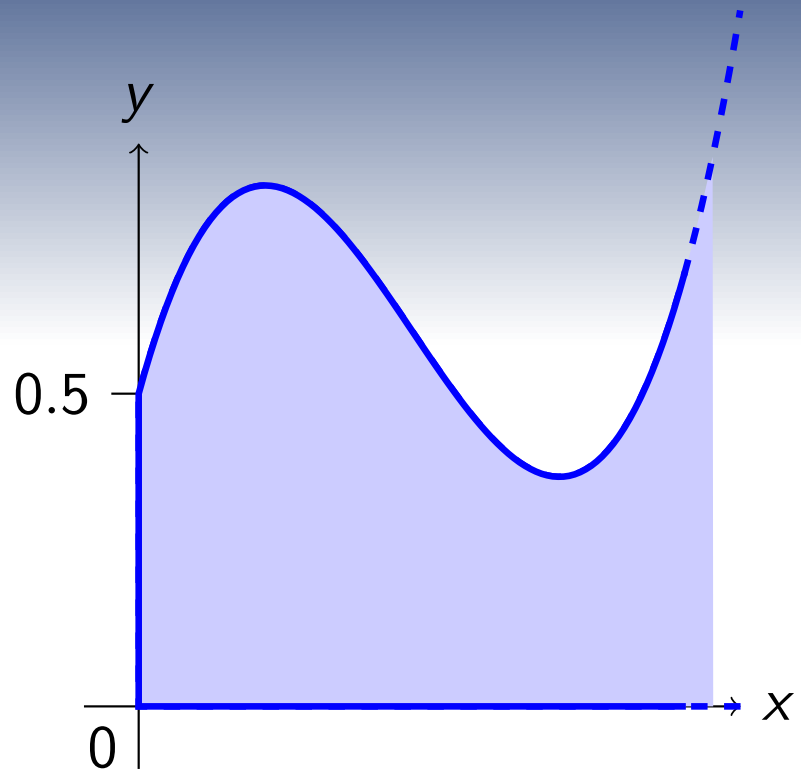
Example



$$(\mathrm{c}) = (0, 0, 0.5, 0, 0.5)$$

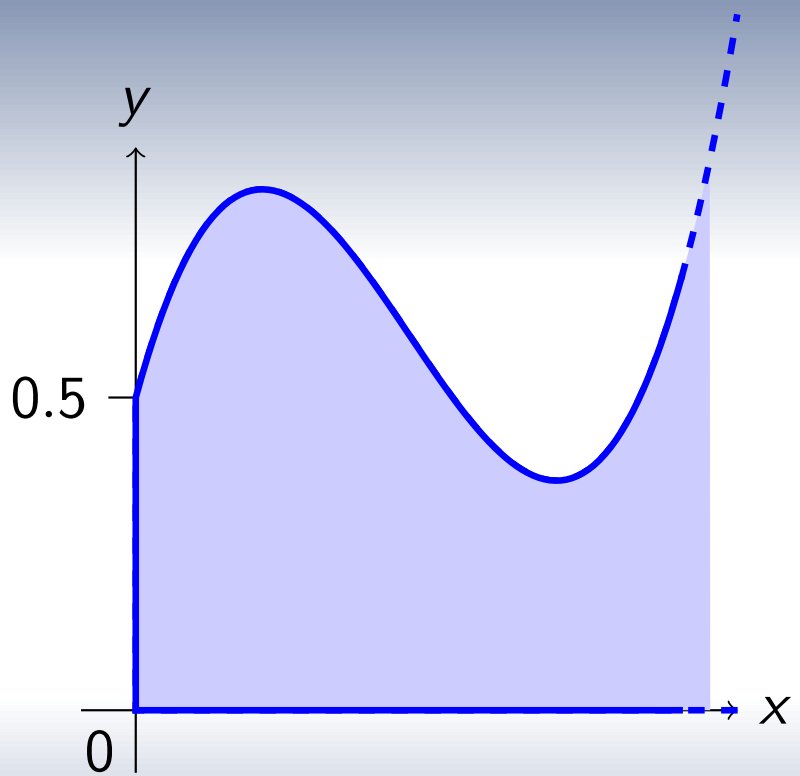


$$(\mathrm{j}) = (0.001, -0.001, 0.503, -0.003, 0.5)$$

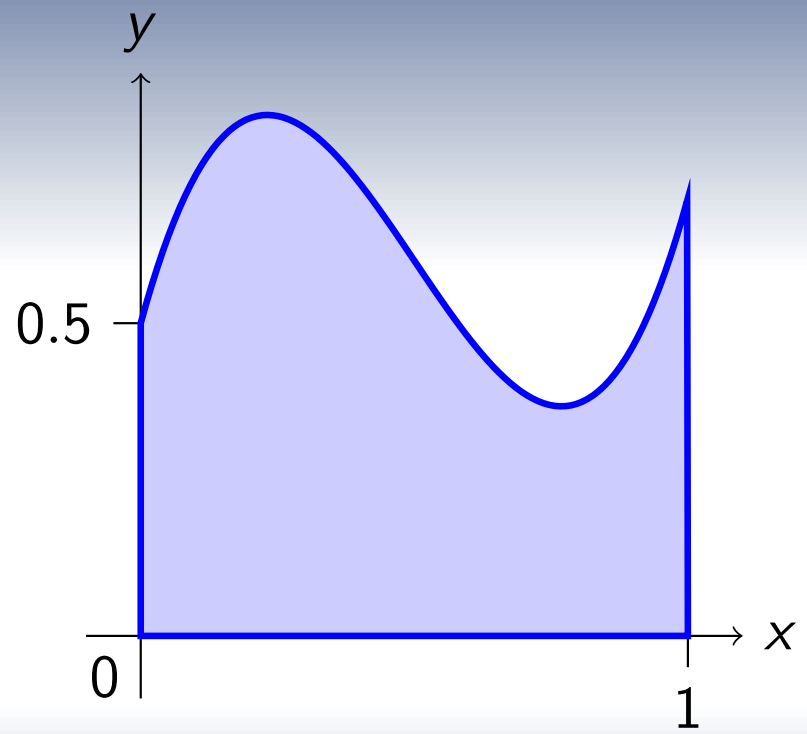


$$(\mathrm{k}) = (\mathrm{c}) \nabla (\mathrm{j}) = (10, 0, 10, 0, 0.5)$$

Example

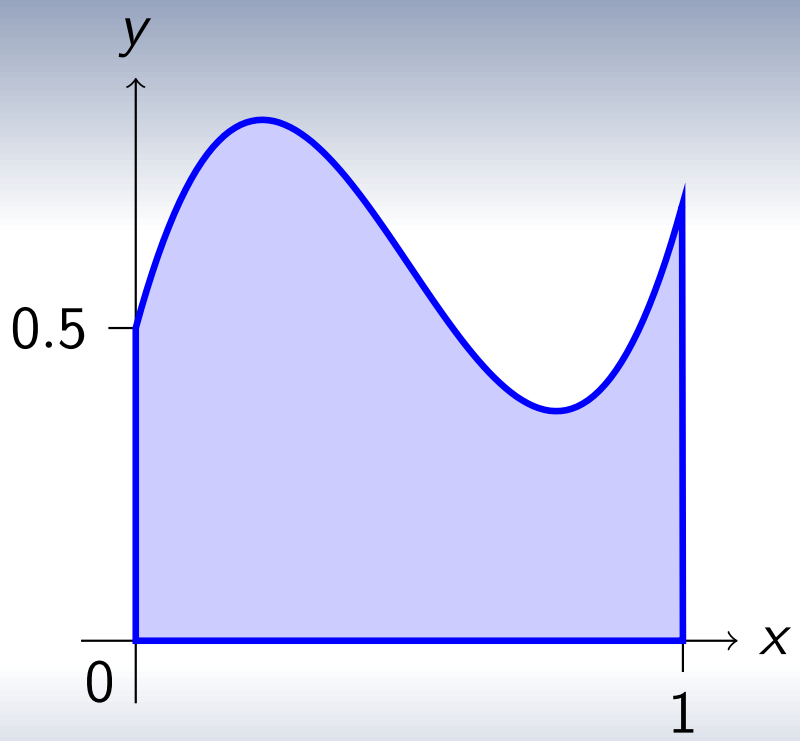


$(\mathrm{k}) = (10, 0, 10, 0, 0.5)$

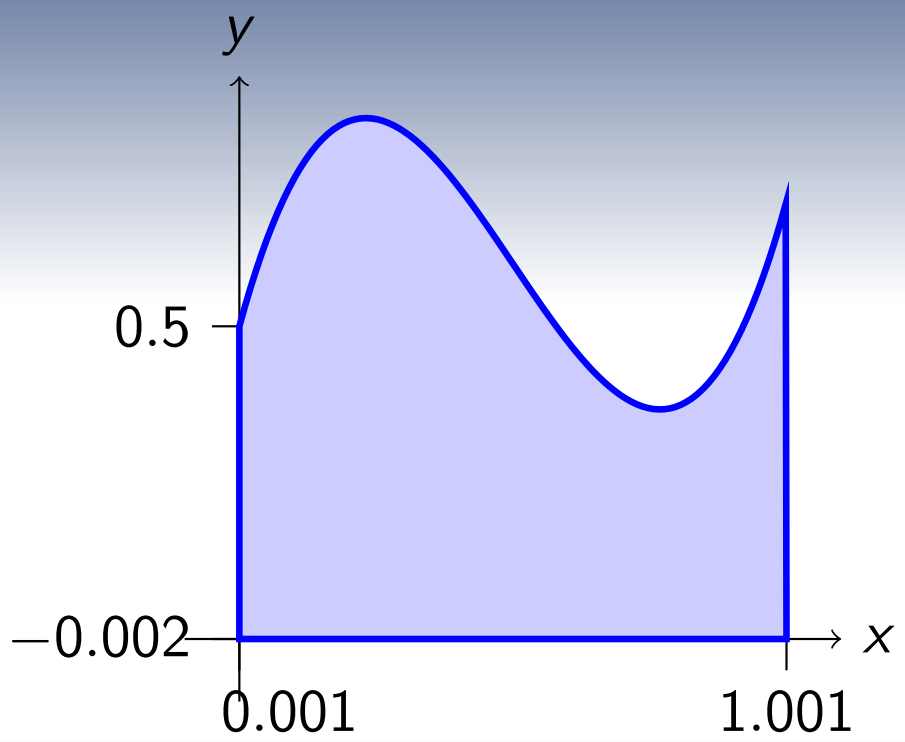


$(\mathrm{l}) = [\![x - 1 \leq 0]\!]^\sharp(\mathrm{k}) =$
$(1, 0, 0.833, 0, 0.5)$

Example

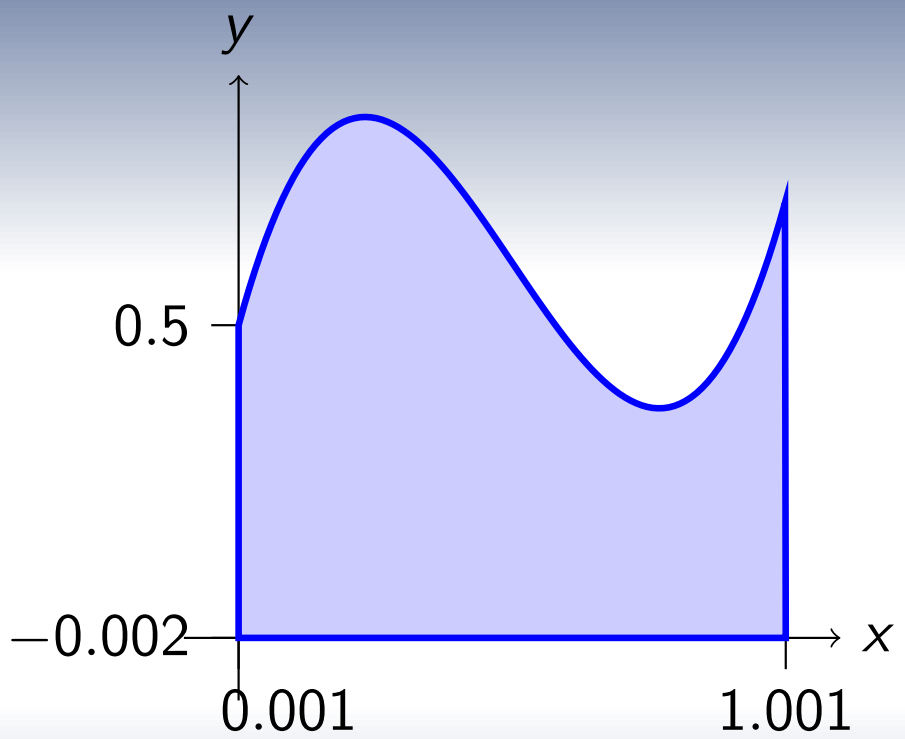


$(\mathrm{l}) = (1, 0, 0.833, 0, 0.5)$

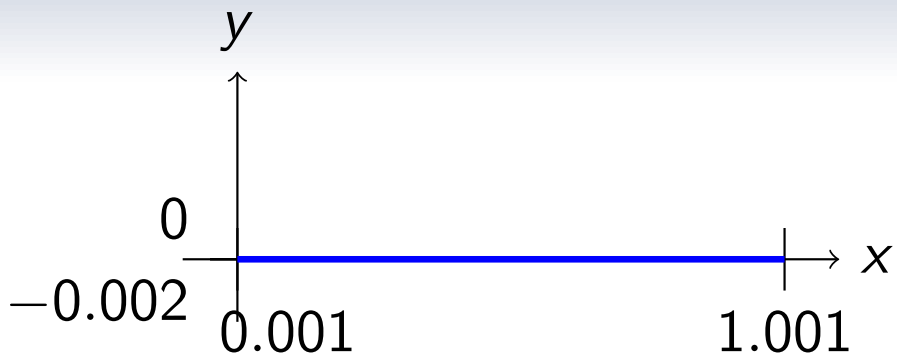


$(\mathrm{m}) = [\![y := y + 0.001(18x^2 - 18x + 3); x := x + 0.001]\!]^\sharp(\mathrm{l}) = (1.001, -0.001, 0.833, 0.002, 0.5)$

Example

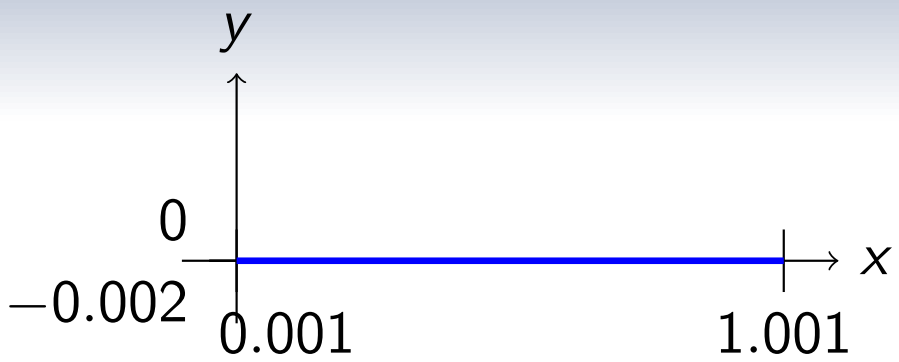


$$(\mathrm{m}) =$$
$$(1.001, -0.001, 0.833, 0.002, 0.5)$$



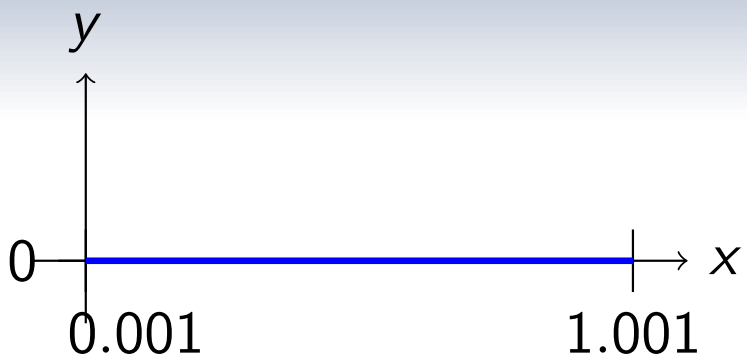
$$(\mathrm{n}) = [\![y \leq 0]\!]^\sharp(\mathrm{m}) =$$
$$(1.001, -0.001, 0, 0.002, 0.133)$$

Example



$(\mathrm{n}) =$

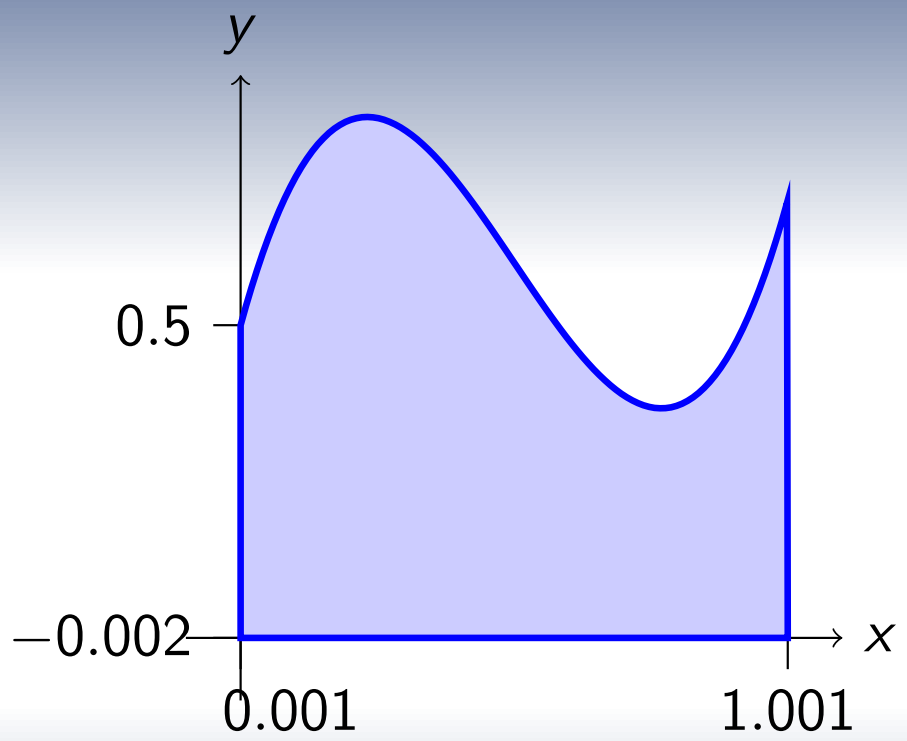
$(1.001, -0.001, 0, 0.002, 0.133)$



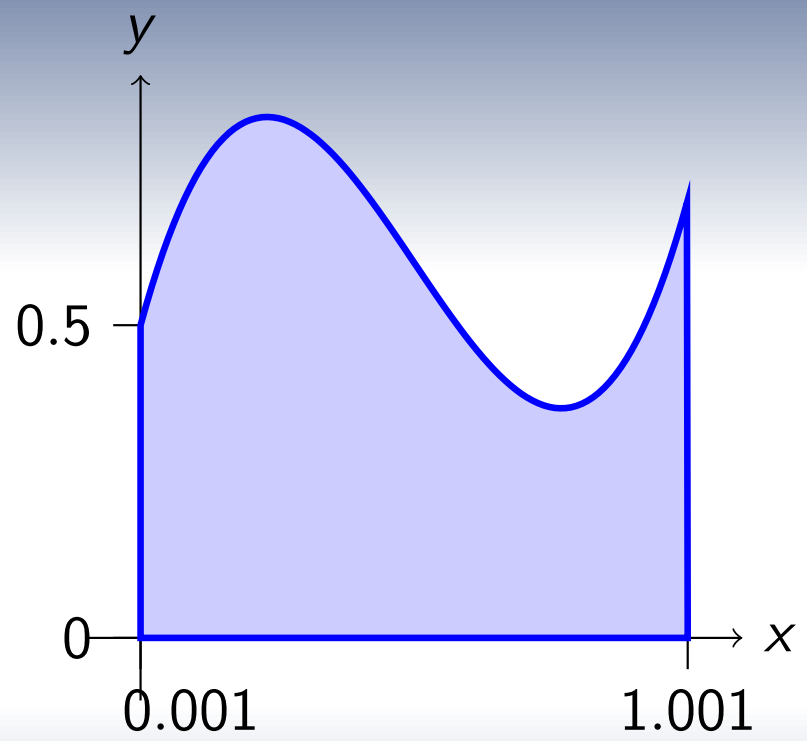
$(\mathrm{o}) = [\![y := 0]\!]^\sharp(\mathrm{n}) =$

$(1.001, -0.001, 0, 0, 0.133)$

Example

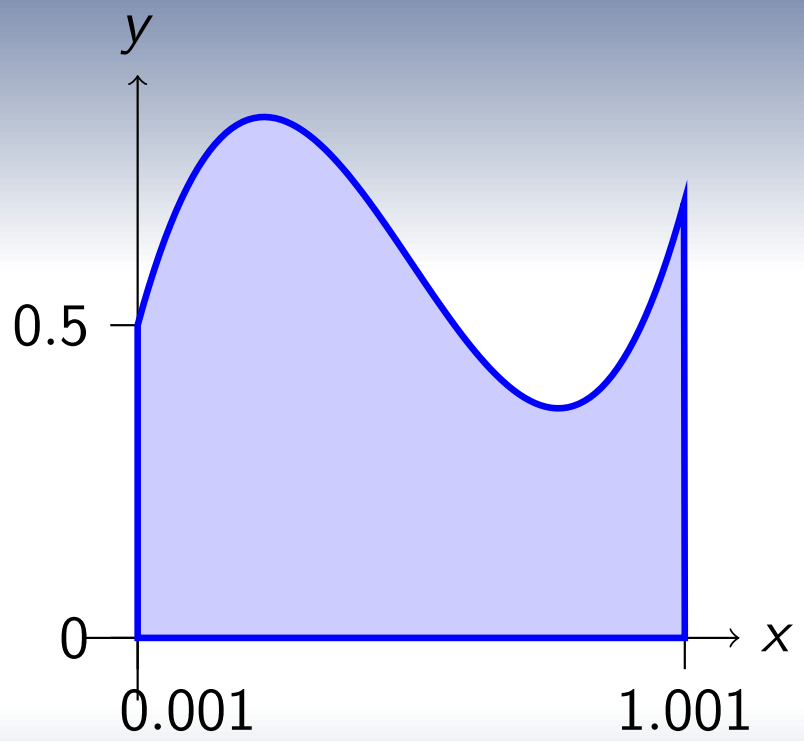


$$(\mathrm{m}) =$$
$$(1.001, -0.001, 0.833, 0.002, 0.5)$$

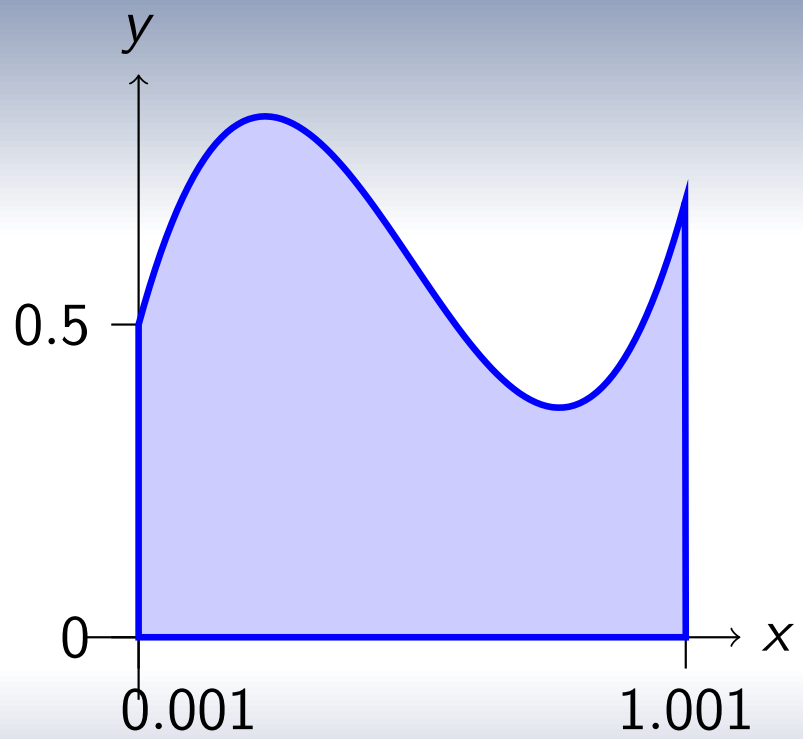


$$(\mathrm{p}) = [\![y \geq 0]\!]^\sharp(\mathrm{m}) =$$
$$(1.001, -0.001, 0.833, 0, 0.5)$$

Example

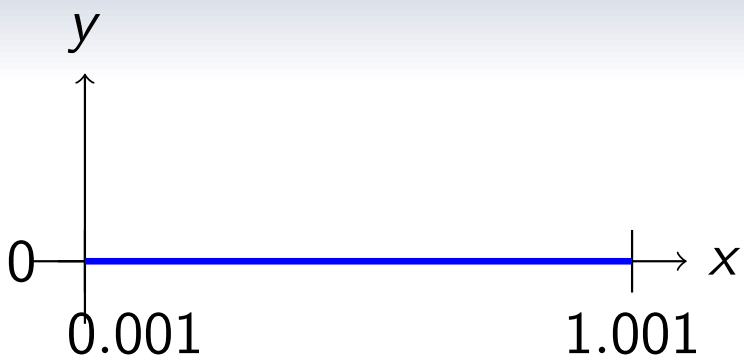


$$(\mathrm{p}) =$$
$$(1.001, -0.001, 0.833, 0, 0.5)$$

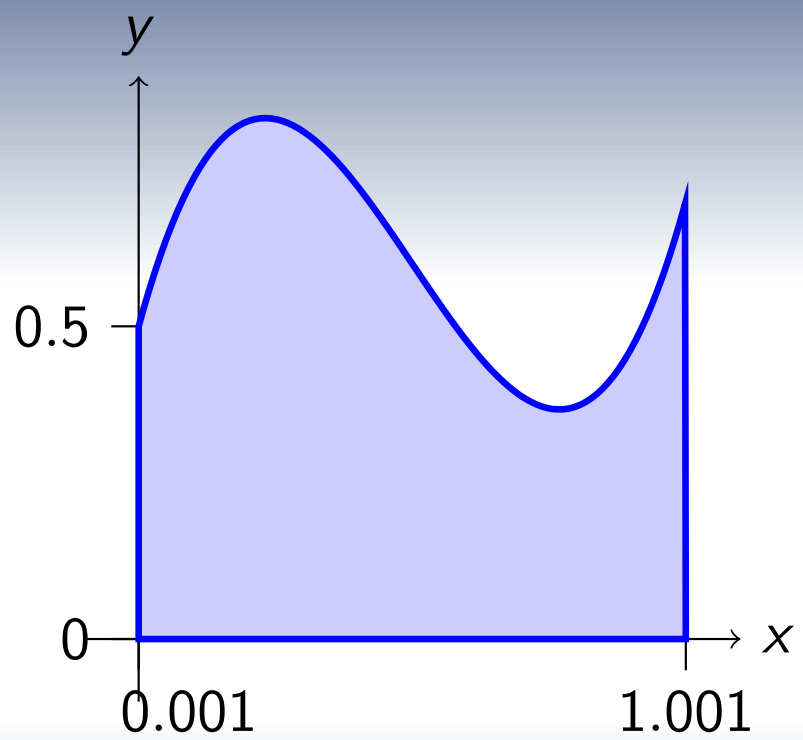


$$(\mathrm{q}) = [\![y := y]\!]^\sharp(\mathrm{p}) = (\mathrm{p})$$

Example



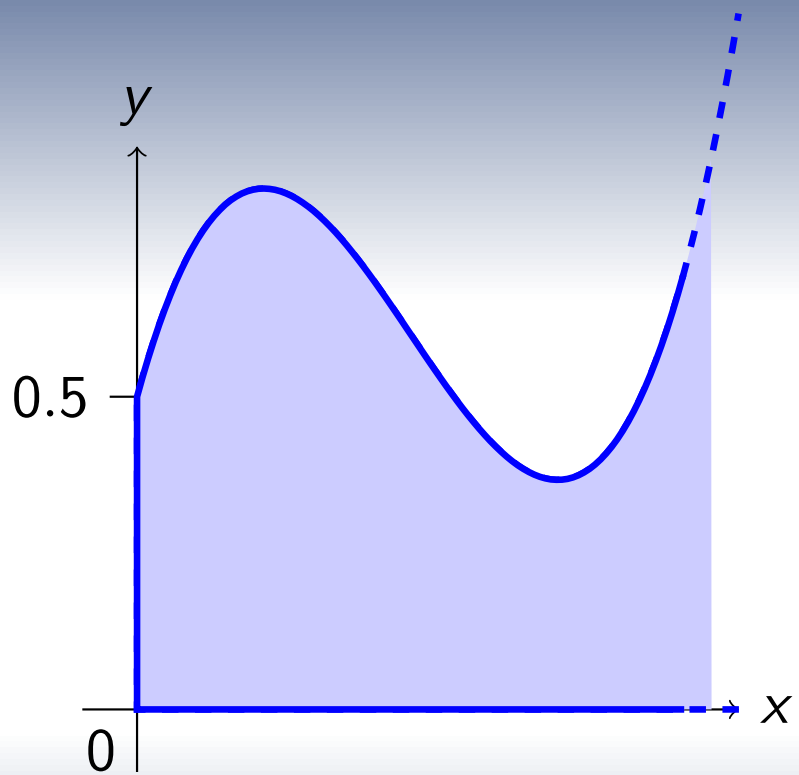
$$(\mathrm{o}) = (1.001, -0.001, 0, 0, 0.133)$$



$$(\mathrm{q}) = (1.001, -0.001, 0.833, 0, 0.5)$$

$$(\mathrm{r}) = (\mathrm{o}) \sqcup^{\sharp} (\mathrm{q}) = (\mathrm{q})$$

Example



$$(\mathrm{k}) = (10, 0, 10, 0, 0.5)$$
$$(\mathrm{r}) = (1.001, -0.001, 0.833, 0, 0.5)$$
$$(\mathrm{s}) = (\mathrm{k}) \nabla (\mathrm{r}) = (\mathrm{k}) \text{ (fixpoint reached!)}$$

Questions

Thank you for your attention!

?