A Weakest Pre–Expectation Semantics for Mixed–Sign Expectations

Benjamin Lucien Kaminski Joost-Pieter Katoen

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

32nd Annual Symposium on **Logic in Computer Science 2017**

June 22, 2017, Reykjavík, Iceland

Example of a Probabilistic Program

$$
\begin{aligned}
&\{c \texttt{ := } 0\}\ [1/2]\ \{c \texttt{ := } 1\};\\
&\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};\\
&\texttt{skip}
\end{aligned}
$$

Example of a Probabilistic Program

$\{c := 0\}\ [1/2]\ \{c := 1\};$ // coin flip

$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$

$\texttt{skip}$

Example of a Probabilistic Program

$\{c := 0\}\ [1/2]\ \{c := 1\};$ // coin flip

$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$

$\texttt{skip}$

What does a probabilistic program C do?

Example of a Probabilistic Program

$$\{c := 0\}\ [1/2]\ \{c := 1\};$$ // coin flip

$$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$$

$$\texttt{skip}$$

What does a probabilistic program C do?

- Run C on initial state $\sigma \in \Sigma$

Example of a Probabilistic Program

$$\{c := 0\}\ [1/2]\ \{c := 1\}; \qquad // \text{ coin flip}$$
$$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$$
$$\texttt{skip}$$

What does a probabilistic program C do?

- Run C on initial state $\sigma \in \Sigma$
- Obtain probability distribution $\llbracket C \rrbracket_\sigma$ over final states

Example of a Probabilistic Program

$$\{c := 0\}\ [1/2]\ \{c := 1\};\qquad // \text{ coin flip}$$
$$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$$
$$\texttt{skip}$$

What does a probabilistic program C do?

- Run C on initial state $\sigma \in \Sigma$
- Obtain probability distribution $[\![C]\!]_\sigma$ over final states

Formal verification of probabilistic programs!

Classical Weakest Pre–Expectations

The Non–Negative Case

Classical Weakest Pre–Expectations

Classical Weakest Pre–Expectations

Expectations:

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f \colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

What we are interested in:

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

What we are interested in:

- Given an expectation f to be evaluated in the final states after termination of a probabilistic program C on input σ

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

What we are interested in:

- Given a post–expectation f to be evaluated in the final states after termination of a probabilistic program C on input σ

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

What we are interested in:

- Given a post–expectation f to be evaluated in the final states after termination of a probabilistic program C on input σ
- Expected value of f after termination of C on σ:

$$\mathsf{EV} \qquad (f)$$

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \to \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

What we are interested in:

- Given a post–expectation f to be evaluated in the final states after termination of a probabilistic program C on input σ
- Expected value of f after termination of C on σ:

$$\mathsf{EV}_{[\![C]\!]_\sigma}(f)$$

Classical Weakest Pre–Expectations

Expectations:

- Expectation is a non–negative random variable $f\colon \Sigma \rightarrow \mathbb{R}_{\geq 0}^{\infty}$
- expectation $\neq$ expected value

What we are interested in:

- Given a post–expectation f to be evaluated in the final states after termination of a probabilistic program C on input σ
- Expected value of f after termination of C on σ:

$$\lambda\sigma\bullet\ \mathsf{EV}_{\llbracket C \rrbracket_\sigma}(f)$$

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C]\colon\ \mathbb{E} \rightarrow \mathbb{E}$.

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C]\colon\ \mathbb{E} \rightarrow \mathbb{E}$.

$$C$$

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C]\colon\ \mathbb{E} \to \mathbb{E}$.

$$C \qquad\qquad f$$

post–expectation f
evaluated in final states
after termination of C

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C] \colon\ \mathbb{E} \rightarrow \mathbb{E}$.

$C \qquad\qquad f$

post–expectation f
evaluated in final states
after termination of C

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C]\colon\ \mathbb{E} \to \mathbb{E}$.

$\mathsf{wp}\,[C]\,(f)$ $\qquad\qquad$ C $\qquad\qquad$ f

post–expectation f
evaluated in final states
after termination of C

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C]\colon\ \mathbb{E} \to \mathbb{E}$.

$\lambda\sigma\text{.}\ \mathsf{EV}_{[\![C]\!]_\sigma}(f) \stackrel{!}{=} \mathsf{wp}\,[C]\,(f)$ $\qquad C \qquad f$

post–expectation f
evaluated in final states
after termination of C

Classical Weakest Preexpectations

The Standard wp Transformer [Kozen, McIver & Morgan]

Use a backward moving expectation transformer $\mathsf{wp}[C]\colon\ \mathbb{E} \to \mathbb{E}$.

$$\lambda\sigma\bullet\ \mathsf{EV}_{[\![C]\!]_\sigma}(f) \stackrel{!}{=} \mathsf{wp}\,[C]\,(f) \qquad C \qquad f$$

weakest pre–expectation
of C with respect to f
evaluated in initial states
before executing C

post–expectation f
evaluated in final states
after termination of C

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$\{c \texttt{ := } 0\}\ [1/2]\ \{c \texttt{ := } 1\}\,;$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

`skip`

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$\{c \mathrel{:=} 0\}\ [1/2]\ \{c \mathrel{:=} 1\}\,;$

$\texttt{if}\ (c = 1)\ \{x \mathrel{:=} 1\}\ \texttt{else}\ \{x \mathrel{:=} 2x + 1\};$

$\texttt{skip}$

x

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$\{c := 0\}\ [1/2]\ \{c := 1\}\,;$

$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$

$\quad \mathsf{wp}\,[\texttt{skip}]\,(x)$

$\texttt{skip}$

$\quad x$

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$\{c \mathrel{:=} 0\} \; [1/2] \; \{c \mathrel{:=} 1\}\,;$

$\texttt{if}\; (c = 1)\; \{x \mathrel{:=} 1\}\; \texttt{else}\; \{x \mathrel{:=} 2x + 1\};$

x

$\texttt{skip}$

x

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$$\{c \texttt{ := } 0\}\ [1/2]\ \{c \texttt{ := } 1\}\,;$$

$$\qquad \mathsf{wp}\,[\texttt{if}\,(c = 1)\ \ldots]\,(x)$$

$$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$$

$$\qquad x$$

$$\texttt{skip}$$

$$\qquad x$$

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$\{c \texttt{ := } 0\}\ [1/2]\ \{c \texttt{ := } 1\}\,;$

$\quad [\![c = 1]\!] \cdot 1 + [\![c = 0]\!] \cdot (2x + 1)$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$\quad x$

$\texttt{skip}$

$\quad x$

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$\{c \texttt{ := } 0\}\ [1/2]\ \{c \texttt{ := } 1\}\,;$

$\quad 1 + [\![c = 0]\!] \cdot 2x$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$\quad x$

$\texttt{skip}$

$\quad x$

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$$\mathsf{wp}\,[\{\ldots\}\;[1/2]\;\{\ldots\}]\,(1 + [\![c = 0]\!] \cdot 2x)$$

$\{c \mathrel{:=} 0\}\;[1/2]\;\{c \mathrel{:=} 1\}\,;$

$$1 + [\![c = 0]\!] \cdot 2x$$

$\texttt{if}\;(c = 1)\;\{x \mathrel{:=} 1\}\;\texttt{else}\;\{x \mathrel{:=} 2x + 1\};$

$$x$$

`skip`

$$x$$

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$$\frac{1}{2} \cdot (1 + [\![0 = 0]\!] \cdot 2x) + \frac{1}{2} \cdot (1 + [\![1 = 0]\!] \cdot 2x)$$

$\{c \texttt{ := } 0\}\ [1/2]\ \{c \texttt{ := } 1\}\,;$

$$1 + [\![c = 0]\!] \cdot 2x$$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$$x$$

$\texttt{skip}$

$$x$$

Weakest Pre–Expectation Reasoning

Example of wp Reasoning

$$1 + x$$

$\{c := 0\}\ [1/2]\ \{c := 1\};$

$$1 + [\![c = 0]\!] \cdot 2x$$

`if` $(c = 1)\ \{x := 1\}$ `else` $\{x := 2x + 1\};$

$$x$$

`skip`

$$x$$

The wp Transformer for While Loops

Use least fixed point construct:

The wp Transformer for While Loops

Use least fixed point construct:

$$\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f) \;=\; \mathsf{lfp}\, F_f(X)$$

The wp Transformer for While Loops

Use least fixed point construct:

$$\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f) \;=\; \mathsf{lfp}\,\underbrace{F_f(X)}_{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot \mathsf{wp}[C](X)}$$

The wp Transformer for While Loops

Use least fixed point construct:

$$\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f) \;=\; \mathsf{lfp}\, \underbrace{F_f(X)}_{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot \mathsf{wp}[C](X)} \;=\; \sup_n \; F_f^n(0)$$

The wp Transformer for While Loops

Use least fixed point construct:

$$\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f) \;=\; \mathsf{lfp}\,\underbrace{F_f(X)}_{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot\mathsf{wp}[C](X)} \;=\; \overbrace{\sup_n \; F_f^n(0)}^{\text{Kleene Fixed Point Theorem}}$$

The wp Transformer for While Loops

Use least fixed point construct:

$$\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f) \;=\; \mathsf{lfp}\,\underbrace{F_f(X)}_{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot \mathsf{wp}[C](X)} \;=\; \overbrace{\sup_n \; F_f^n(0)}^{\text{Kleene Fixed Point Theorem}}$$

Complete partial order on expectations:

$$f_1 \;\preceq\; f_2 \quad \text{iff} \quad \forall \sigma\colon f_1(\sigma) \;\leq\; f_2(\sigma)$$

The Motivation

Example of wp Reasoning

$$1 + x$$

$\texttt{if}\ (1/2)\ \{c \texttt{ := } 0\}\ \texttt{else}\ \{c \texttt{ := } 1\};$

$$1 + [\![c = 0]\!] \cdot 2x$$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$$x$$

`skip`

$$x$$

The Motivation

Example of wp Reasoning

$$1 + x \not\in \mathbb{E}$$

$\texttt{if}\ (1/2)\ \{c \texttt{ := } 0\}\ \texttt{else}\ \{c \texttt{ := } 1\};$

$$1 + [\![c = 0]\!] \cdot 2x \not\in \mathbb{E}$$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$$x \not\in \mathbb{E}$$

`skip`

$$x \not\in \mathbb{E}$$

The Motivation

Example of wp Reasoning

$$1 + x \not\in \mathbb{E}$$

$\texttt{if}\ (1/2)\ \{c \texttt{ := } 0\}\ \texttt{else}\ \{c \texttt{ := } 1\};$

$$1 + [\![c = 0]\!] \cdot 2x \not\in \mathbb{E}$$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$$x \not\in \mathbb{E}$$

`skip`

$$x \not\in \mathbb{E}$$

Neither post–expectation x nor any of the pre–expectations are p<u>ro</u>p<u>er</u> expectations!

Mixed–Sign Weakest Pre–Expectations

The Non–Non–Negative Case

Our Solution: Integrability–Witnessing Expectations

Our Solution: Integrability–Witnessing Expectations

- Define set of mixed–sign expectations $\mathbb{E}^\star = \{f \mid f\colon \Sigma \to \mathbb{R}\}$

Our Solution: Integrability–Witnessing Expectations

- Define set of mixed–sign expectations $\mathbb{E}^\star = \{f \mid f\colon \Sigma \to \mathbb{R}\}$
- **EV(f) is well–defined if and only if EV$\big(|f|\big) < \infty$**

Our Solution: Integrability–Witnessing Expectations

- Define set of mixed–sign expectations $\mathbb{E}^{\star} = \{f \mid f\colon \Sigma \to \mathbb{R}\}$
- **EV(f) is well–defined if and only if EV$\big(|f|\big) < \infty$**
  - In probability theory terms: f should be integrable

Our Solution: Integrability–Witnessing Expectations

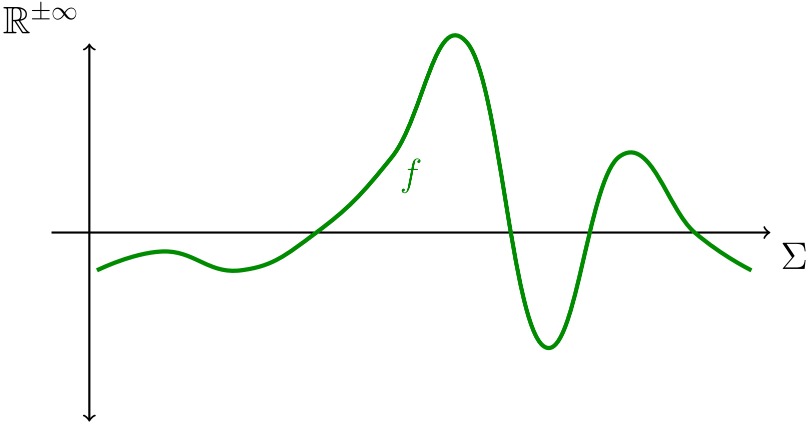
- Define set of mixed–sign expectations $\mathbb{E}^\star = \{f \mid f\colon \Sigma \to \mathbb{R}\}$
- **EV(f) is well–defined if and only if EV$\big(|f|\big) < \infty$**
  - In probability theory terms: f should be integrable
- Integrability–witnessing pairs:

$$(f,\, g)$$

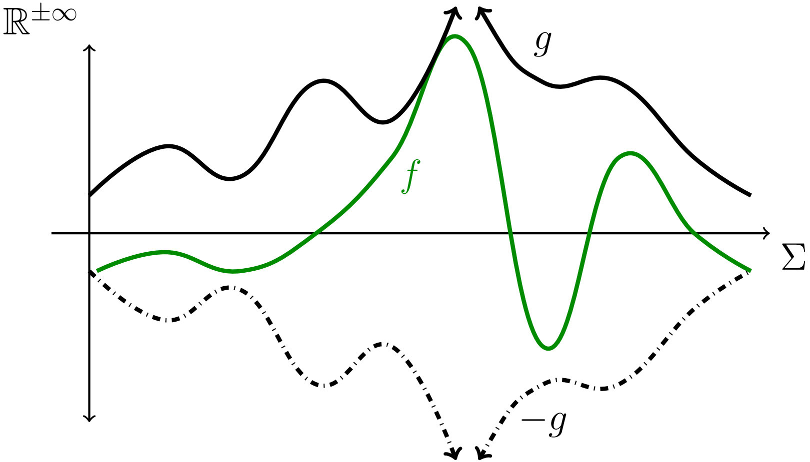
such that $f \in \mathbb{E}^\star$, $g \in \mathbb{E}$, and $|f| \leq g$

Our Solution: Integrability–Witnessing Expectations

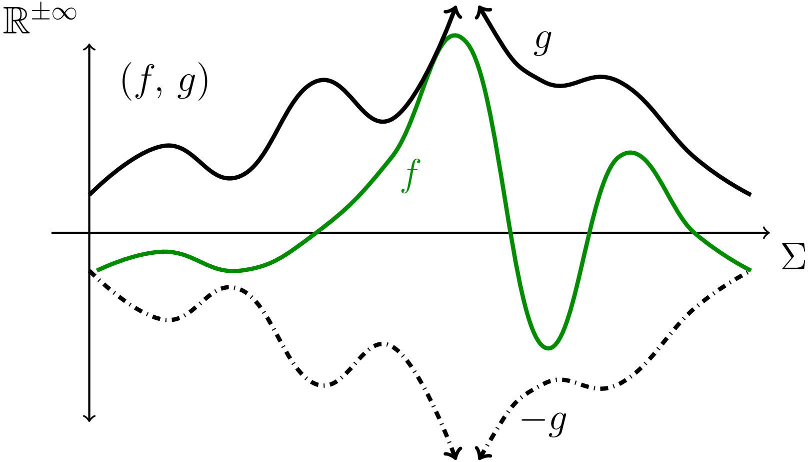
Our Solution: Integrability–Witnessing Expectations



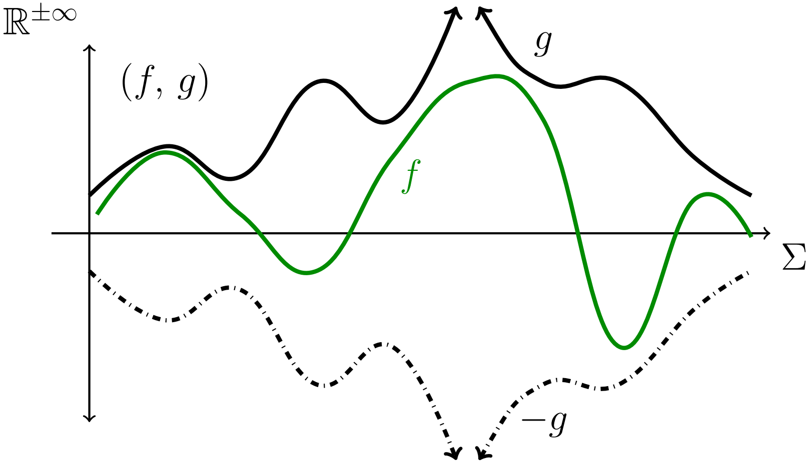
Our Solution: Integrability–Witnessing Expectations



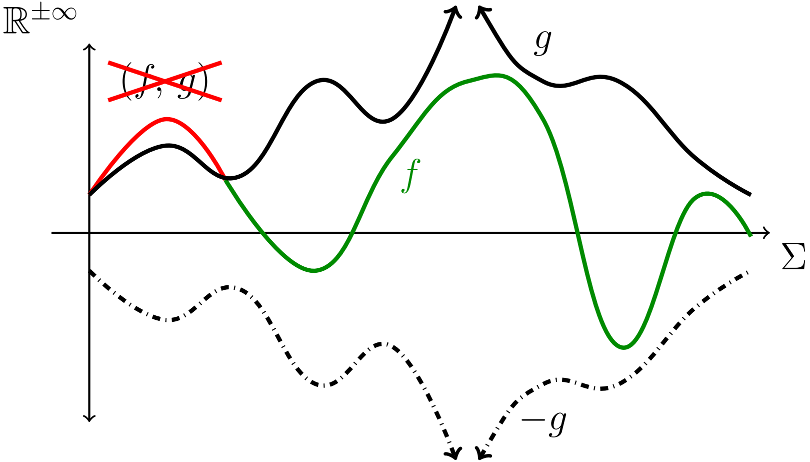
Our Solution: Integrability–Witnessing Expectations



Our Solution: Integrability–Witnessing Expectations



Our Solution: Integrability–Witnessing Expectations



wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$\texttt{if}\ (1/2)\ \{c\ \texttt{:=}\ 0\}\ \texttt{else}\ \{c\ \texttt{:=}\ 1\};$

$\texttt{if}\ (c = 1)\ \{x\ \texttt{:=}\ 1\}\ \texttt{else}\ \{x\ \texttt{:=}\ 2x + 1\};$

$\texttt{skip}$

wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$\texttt{if}\ (1/2)\ \{c := 0\}\ \texttt{else}\ \{c := 1\};$

$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$

$\texttt{skip}$

$\quad (x,\ |x|)$

wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$\texttt{if}\ (1/2)\ \{c\ \texttt{:=}\ 0\}\ \texttt{else}\ \{c\ \texttt{:=}\ 1\};$

$\texttt{if}\ (c = 1)\ \{x\ \texttt{:=}\ 1\}\ \texttt{else}\ \{x\ \texttt{:=}\ 2x+1\};$

$\quad \left(\mathsf{wp}\,[\texttt{skip}]\,(x)\,,\ \mathsf{wp}\,[\texttt{skip}]\,(|x|)\right)$

$\texttt{skip}$

$\quad (x,\ |x|)$

wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$\texttt{if}\ (1/2)\ \{c \texttt{ := } 0\}\ \texttt{else}\ \{c \texttt{ := } 1\};$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$\quad (x,\ |x|)$

$\texttt{skip}$

$\quad (x,\ |x|)$

wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$\texttt{if}\;(1/2)\;\{c := 0\}\;\texttt{else}\;\{c := 1\};$

$\quad\big(\mathsf{wp}\,[\texttt{if}(c = 1)\;\ldots]\,(x)\,,\;\mathsf{wp}\,[\texttt{if}(c = 1)\;\ldots]\,(|x|)\,\big)$

$\texttt{if}\;(c = 1)\;\{x := 1\}\;\texttt{else}\;\{x := 2x + 1\};$

$\quad\big(x,\;|x|\big)$

$\texttt{skip}$

$\quad\big(x,\;|x|\big)$

wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$\texttt{if}\ (1/2)\ \{c \texttt{ := } 0\}\ \texttt{else}\ \{c \texttt{ := } 1\};$

$\quad \big(1 + [\![c = 0]\!] \cdot 2x,\ [\![c = 1]\!] + [\![c = 0]\!] \cdot |2x + 1|\big)$

$\texttt{if}\ (c = 1)\ \{x \texttt{ := } 1\}\ \texttt{else}\ \{x \texttt{ := } 2x + 1\};$

$\quad \big(x,\ |x|\big)$

$\texttt{skip}$

$\quad \big(x,\ |x|\big)$

wp with Integrability–Witnessing Pairs

Example of Integrability–Witnessing Pair Reasoning

$$\left(1 + x,\ \frac{1}{2} + \left|x + \frac{1}{2}\right|\right)$$

$\texttt{if}\ (1/2)\ \{c := 0\}\ \texttt{else}\ \{c := 1\};$

$$\big(1 + [\![c = 0]\!] \cdot 2x,\ [\![c = 1]\!] + [\![c = 0]\!] \cdot |2x + 1|\big)$$

$\texttt{if}\ (c = 1)\ \{x := 1\}\ \texttt{else}\ \{x := 2x + 1\};$

$$\big(x,\ |x|\big)$$

$\texttt{skip}$

$$\big(x,\ |x|\big)$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall $\mathsf{wp}\,[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall wp $[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

What about Loops?

- Consider `while` (ξ) $\{C\}$
- Recall wp $[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0) \right)$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall wp $[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \triangleright \quad \texttt{while}\,(1/2)\,\{\; x := -2 \cdot x \}$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall wp $[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \;\triangleright\; \qquad \texttt{while}\,(1/2)\,\{ \\ x := -2 \cdot x\}$$

- According sequence:

What about Loops?

- Consider `while` (ξ) $\{C\}$
- Recall wp $[\texttt{while}\ (\xi)\ \{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \triangleright \qquad \texttt{while}\ (1/2)\ \{\ x := -2 \cdot x \}$$

- According sequence:

$$\left(\frac{x}{2}, \frac{|x|}{2} \right)$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall $\mathsf{wp}\,[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \triangleright \qquad \begin{array}{l} \texttt{while}\,(1/2)\,\{ \\ \qquad x := -2 \cdot x\} \end{array}$$

- According sequence:

$$\left(\frac{x}{2},\, \frac{|x|}{2} \right) \quad \left(0,\, |x| \right)$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall wp $[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0)\right)$$

- Consider the program

$$C_{geo2} \triangleright \qquad \texttt{while}\ (1/2)\ \{ \\ x := -2 \cdot x\}$$

- According sequence:

$$\left(\frac{x}{2}, \frac{|x|}{2}\right) \quad \left(0, |x|\right) \quad \left(\frac{x}{2}, \frac{3|x|}{2}\right)$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall wp $[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\ F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \;\triangleright\; \qquad \texttt{while}\,(1/2)\,\{\; x := -2 \cdot x \}$$

- According sequence:

$$\left(\frac{x}{2},\, \frac{|x|}{2}\right) \quad \left(0,\, |x|\right) \quad \left(\frac{x}{2},\, \frac{3|x|}{2}\right) \quad \left(0,\, 2|x|\right)$$

What about Loops?

- Consider $\texttt{while}\ (\xi)\ \{C\}$
- Recall wp $[\texttt{while}\ (\xi)\ \{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\ F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \ \triangleright \qquad \texttt{while}\ (1/2)\ \{ \\ x := -2 \cdot x \}$$

- According sequence:

$$\left(\frac{x}{2},\ \frac{|x|}{2}\right) \quad \Big(0,\ |x|\Big) \quad \left(\frac{x}{2},\ \frac{3|x|}{2}\right) \quad \Big(0,\ 2|x|\Big) \quad \cdots$$

What about Loops?

- Consider `while` $(\xi)\ \{C\}$
- Recall wp $[\texttt{while}\ (\xi)\ \{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\ F_{|f|}^n(0) \right)$$

- Consider the program

$$C_{geo2} \triangleright \qquad \texttt{while}\ (1/2)\ \{\ x := -2 \cdot x \}$$

- According sequence:

$$\left(\frac{x}{2},\ \frac{|x|}{2} \right) \quad \left(0,\ |x| \right) \quad \left(\frac{x}{2},\ \frac{3|x|}{2} \right) \quad \left(0,\ 2|x| \right) \quad \cdots$$

What about Loops?

- Consider $\texttt{while}\,(\xi)\,\{C\}$
- Recall $\mathsf{wp}\,[\texttt{while}\,(\xi)\,\{C\}]\,(f) = \sup_n F_f^n(0)$ (KFPT)
- Can we do KFPT–style approximations of loop semantics using integrability–witnessing pairs?

$$\lim_{n \to \omega} \left(F_f^n(0),\, F_{|f|}^n(0) \right)$$

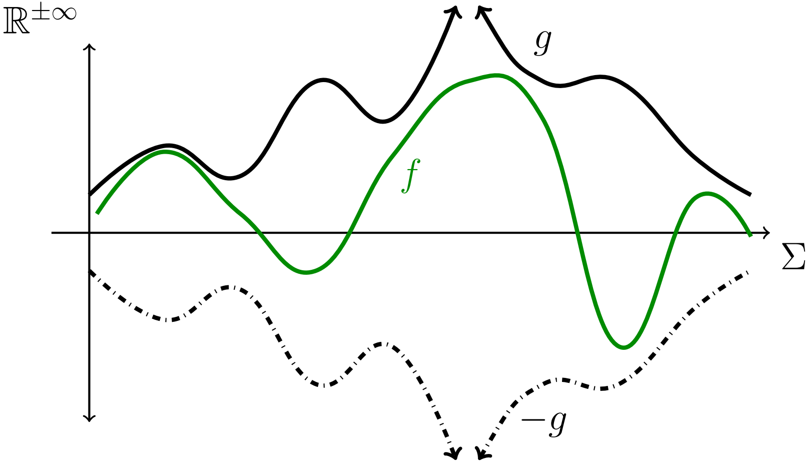
- Consider the program

$$C_{geo2} \;\triangleright\; \qquad \begin{array}{l} \texttt{while}\,(1/2)\,\{ \\ \qquad x := -2 \cdot x\} \end{array}$$

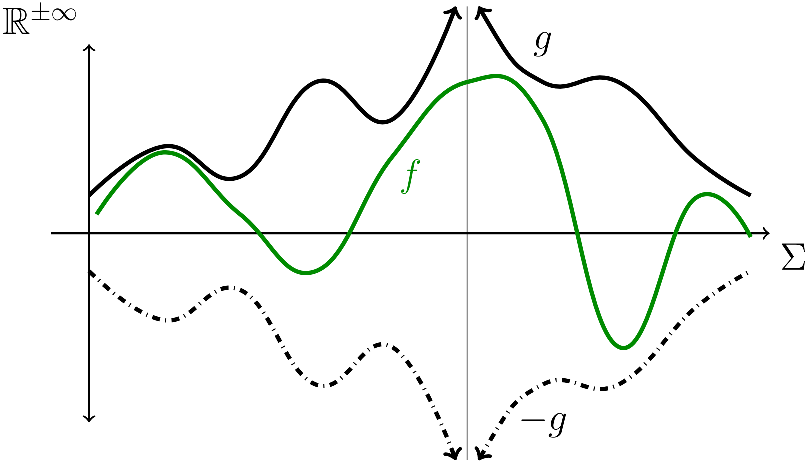
- According sequence:

$$\left(\frac{x}{2},\, \frac{|x|}{2}\right) \quad \left(0,\, |x|\right) \quad \left(\frac{x}{2},\, \frac{3|x|}{2}\right) \quad \left(0,\, 2|x|\right) \quad \cdots$$ ☹ ?

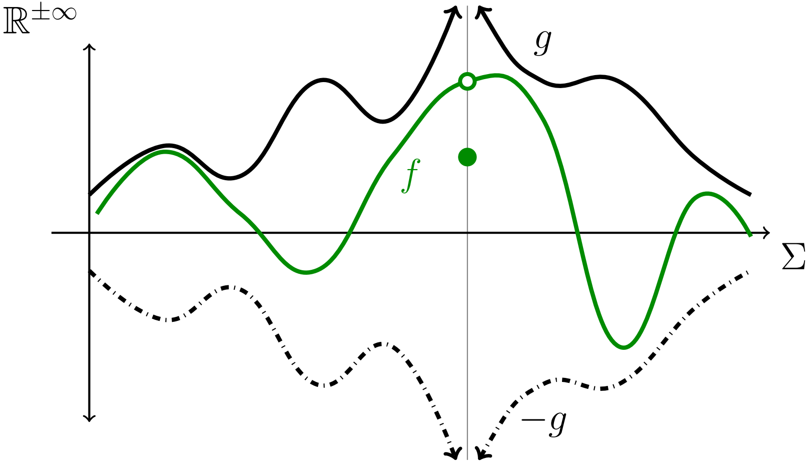
Our Solution: Integrability–Witnessing Expectations



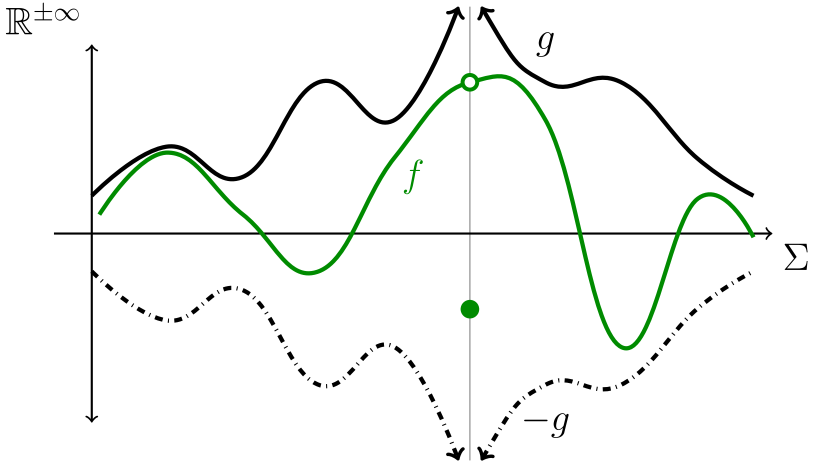
Our Solution: Integrability–Witnessing Expectations



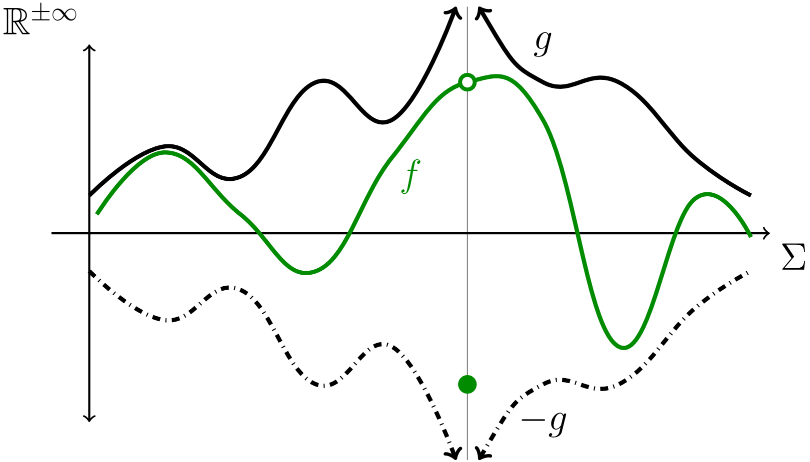
Our Solution: Integrability–Witnessing Expectations



Our Solution: Integrability–Witnessing Expectations



Our Solution: Integrability–Witnessing Expectations



Our Solution: Integrability–Witnessing Expectations

Our Solution: Integrability–Witnessing Expectations

- equivalence relation $\approx$ on pairs: $(f_1,\, g) \approx (f_2,\, g)$ iff

$$\forall \sigma\colon \qquad g(\sigma) \;\neq\; \infty \quad \text{implies} \quad f_1(\sigma) \;=\; f_2(\sigma)$$

Our Solution: Integrability–Witnessing Expectations

- equivalence relation $\approx$ on pairs: $(f_1,\, g) \approx (f_2,\, g)$ iff

$$\forall \sigma: \qquad g(\sigma) \neq \infty \quad \text{implies} \quad f_1(\sigma) = f_2(\sigma)$$

- Integrability–witnessing expectation (IWE):

  $\approx$–equivalence class $\wr f,\, g \int$ of $(f,\, g)$

Our Solution: Integrability–Witnessing Expectations

- equivalence relation $\approx$ on pairs: $(f_1,\, g) \approx (f_2,\, g)$ iff

$$\forall \sigma: \qquad g(\sigma) \;\neq\; \infty \quad \text{implies} \quad f_1(\sigma) \;=\; f_2(\sigma)$$

- Integrability–witnessing expectation (IWE):

  $\approx$–equivalence class $\wr f,\, g \int$ of $(f,\, g)$

- partial order on IWEs: $\wr f,\, g \int \sqsubseteq \wr f',\, g' \int$ iff

$$\forall \sigma: \qquad g'(\sigma) \;\neq\; \infty \quad \text{implies} \quad f(\sigma) \leq f'(\sigma) \text{ and } g(\sigma) \leq g'(\sigma)$$

Our Solution: Integrability–Witnessing Expectations

- equivalence relation $\approx$ on pairs: $(f_1,\, g) \approx (f_2,\, g)$ iff

$$\forall \sigma : \qquad g(\sigma) \;\neq\; \infty \quad \text{implies} \quad f_1(\sigma) \;=\; f_2(\sigma)$$

- Integrability–witnessing expectation (IWE):

  $\approx$–equivalence class $\wr f,\, g \int$ of $(f,\, g)$

- partial order on IWEs: $\wr f,\, g \int \sqsubseteq \wr f',\, g' \int$ iff

$$\forall \sigma : \qquad g'(\sigma) \;\neq\; \infty \quad \text{implies} \quad f(\sigma) \leq f'(\sigma) \text{ and } g(\sigma) \leq g'(\sigma)$$

- $\sqsubseteq$ is not a cpo. No least element! In particular:

$$\wr 0,\, 0 \int \;\not\sqsubseteq\; \wr -1,\, 1 \int$$

Our Solution: Integrability–Witnessing Expectations

- equivalence relation $\approx$ on pairs: $(f_1,\, g) \approx (f_2,\, g)$ iff

$$\forall \sigma: \qquad g(\sigma) \;\neq\; \infty \quad \text{implies} \quad f_1(\sigma) \;=\; f_2(\sigma)$$

- Integrability–witnessing expectation (IWE):

  $\approx$–equivalence class $\wr f,\, g \int$ of $(f,\, g)$

- partial order on IWEs: $\wr f,\, g \int \sqsubseteq \wr f',\, g' \int$ iff

$$\forall \sigma: \qquad g'(\sigma) \;\neq\; \infty \quad \text{implies} \quad f(\sigma) \leq f'(\sigma) \text{ and } g(\sigma) \leq g'(\sigma)$$

- $\sqsubseteq$ is not a cpo. No least element! In particular:

$$\wr 0,\, 0 \int \;\not\sqsubseteq\; \wr -1,\, 1 \int$$

- Still we can define a wp transformer acting on IWEs

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g \wr \;=\; \lim_{n \to \omega}\; F^{n}_{\wr f,\, g \wr}\,\wr 0,\, 0 \wr$$

$$F_{\wr f,\, g \wr}\,\wr X,\, Y \wr \;=\; [\![\neg \xi]\!] \cdot \wr f,\, g \wr + [\![\xi]\!] \cdot \mathsf{wp}[C]\wr X,\, Y \wr$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g\wr \;=\; \lim_{n\to\omega}\; F^{n}_{\wr f,\, g\wr}\wr 0,\, 0\wr$$

$$F_{\wr f,\, g\wr}\wr X,\, Y\wr \;=\; [\![\neg\xi]\!]\cdot\wr f,\, g\wr + [\![\xi]\!]\cdot\mathsf{wp}[C]\wr X,\, Y\wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\; \begin{array}{l}\mathtt{while}\;({}^{1}\!/_{2})\;\{\\ \qquad x := -2\cdot x\}\end{array}$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g\wr \;=\; \lim_{n\to\omega}\; F^{n}_{\wr f,\, g\wr}\,\wr 0,\, 0\wr$$

$$F_{\wr f,\, g\wr}\,\wr X,\, Y\wr \;=\; [\![\neg\xi]\!]\cdot \wr f,\, g\wr + [\![\xi]\!]\cdot \mathtt{wp}[C]\wr X,\, Y\wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\; \quad \mathtt{while}\;(1/2)\;\{ \;\; x := -2\cdot x\}$$

- According sequence $F^{n}_{\wr f,\, g\wr}\,\wr 0,\, 0\wr$:

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g\wr \;=\; \lim_{n\to\omega}\; F^{n}_{\wr f,\, g\wr}\wr 0,\, 0\wr$$

$$F_{\wr f,\, g\wr}\wr X,\, Y\wr \;=\; [\![\neg\xi]\!]\cdot\wr f,\, g\wr + [\![\xi]\!]\cdot \mathtt{wp}[C]\wr X,\, Y\wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\qquad \mathtt{while}\;(1/2)\;\{\; x := -2\cdot x\}$$

- According sequence $F^{n}_{\wr f,\, g\wr}\wr 0,\, 0\wr$:

$$\wr \frac{x}{2},\, \frac{|x|}{2} \wr$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g \wr \;=\; \lim_{n \to \omega} F^{n}_{\wr f,\, g \wr} \wr 0,\, 0 \wr$$

$$F_{\wr f,\, g \wr} \wr X,\, Y \wr \;=\; [\![\neg \xi]\!] \cdot \wr f,\, g \wr + [\![\xi]\!] \cdot \mathtt{wp}[C] \wr X,\, Y \wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\; \quad \mathtt{while}\;(1/2)\;\{\; x := -2 \cdot x \}$$

- According sequence $F^{n}_{\wr f,\, g \wr} \wr 0,\, 0 \wr$:

$$\wr \tfrac{x}{2},\, \tfrac{|x|}{2} \wr \quad \wr 0,\, |x| \wr$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g \wr \;=\; \lim_{n \to \omega} F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$$

$$F_{\wr f,\, g \wr} \wr X,\, Y \wr \;=\; [\![\neg \xi]\!] \cdot \wr f,\, g \wr + [\![\xi]\!] \cdot \mathsf{wp}[C] \wr X,\, Y \wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright \qquad \mathtt{while}\ (1/2)\ \{\; x := -2 \cdot x\}$$

- According sequence $F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$:

$$\wr \frac{x}{2},\, \frac{|x|}{2} \wr \quad \wr 0,\, |x| \wr \quad \wr \frac{x}{2},\, \frac{3|x|}{2} \wr$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g \wr \;=\; \lim_{n\to\omega}\; F^{n}_{\wr f,\, g \wr}\wr 0,\, 0 \wr$$

$$F_{\wr f,\, g \wr}\wr X,\, Y \wr \;=\; [\![\neg\xi]\!]\cdot \wr f,\, g \wr + [\![\xi]\!]\cdot \mathtt{wp}[C]\wr X,\, Y \wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\; \qquad \mathtt{while}\;(1/2)\;\{\; x := -2\cdot x \}$$

- According sequence $F^{n}_{\wr f,\, g \wr}\wr 0,\, 0 \wr$:

$$\left\wr \frac{x}{2},\, \frac{|x|}{2} \right\wr \;\; \left\wr 0,\, |x| \right\wr \;\; \left\wr \frac{x}{2},\, \frac{3|x|}{2} \right\wr \;\; \left\wr 0,\, 2|x| \right\wr$$

IWEs and Loops

$$\mathsf{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g \wr \;=\; \lim_{n \to \omega} F^{n}_{\wr f,\, g \wr} \wr 0,\, 0 \wr$$

$$F_{\wr f,\, g \wr} \wr X,\, Y \wr \;=\; [\![\neg \xi]\!] \cdot \wr f,\, g \wr + [\![\xi]\!] \cdot \mathsf{wp}[C] \wr X,\, Y \wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\; \quad \mathtt{while}\;(1/2)\;\{\; x := -2 \cdot x \}$$

- According sequence $F^{n}_{\wr f,\, g \wr} \wr 0,\, 0 \wr$:

$$\wr \tfrac{x}{2},\, \tfrac{|x|}{2} \wr \quad \wr 0,\, |x| \wr \quad \wr \tfrac{x}{2},\, \tfrac{3|x|}{2} \wr \quad \wr 0,\, 2|x| \wr$$

IWEs and Loops

$$\mathsf{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g\wr \;=\; \lim_{n\to\omega}\; F^n_{\wr f,\, g\wr}\wr 0,\, 0\wr$$

$$F_{\wr f,\, g\wr}\wr X,\, Y\wr \;=\; [\![\neg\xi]\!]\cdot\wr f,\, g\wr + [\![\xi]\!]\cdot \mathsf{wp}[C]\wr X,\, Y\wr$$

- Reconsider the program

$$C_{geo2} \;\rhd\qquad \mathtt{while}\;(1/2)\;\{\; x := -2\cdot x\}$$

- According sequence $F^n_{\wr f,\, g\wr}\wr 0,\, 0\wr$:

$$\wr \frac{x}{2}, \frac{|x|}{2}\wr \;\; \wr 0,\, |x|\wr \;\; \wr \frac{x}{2}, \frac{3|x|}{2}\wr \;\; \wr 0,\, 2|x|\wr \;\; \cdots \xrightarrow{\;\omega\;} \;\; \wr 0\,,\, \infty\cdot|x|\wr$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g\wr \;=\; \lim_{n\to\omega}\; F^{n}_{\wr f,\, g\wr}\wr 0,\, 0\wr$$

$$F_{\wr f,\, g\wr}\wr X,\, Y\wr \;=\; [\![\neg\xi]\!]\cdot\wr f,\, g\wr + [\![\xi]\!]\cdot \mathtt{wp}[C]\wr X,\, Y\wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\qquad \mathtt{while}\;(1/2)\;\{\; x := -2\cdot x\}$$

- According sequence $F^{n}_{\wr f,\, g\wr}\wr 0,\, 0\wr$:

$$\wr \frac{x}{2}, \frac{|x|}{2}\wr \quad \wr 0,\, |x|\wr \quad \wr \frac{x}{2}, \frac{3|x|}{2}\wr \quad \wr 0,\, 2|x|\wr \quad \cdots \xrightarrow{\omega} \quad \wr \frac{x}{2}, \infty\cdot|x|\wr$$

IWEs and Loops

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C\}]\wr f,\, g \wr \;=\; \lim_{n \to \omega} F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$$

$$F_{\wr f,\, g \wr} \wr X,\, Y \wr \;=\; [\![\neg \xi]\!] \cdot \wr f,\, g \wr + [\![\xi]\!] \cdot \mathtt{wp}[C] \wr X,\, Y \wr$$

- Reconsider the program

$$C_{geo2} \;\triangleright\; \quad \mathtt{while}\,(1/2)\,\{\; x := -2 \cdot x \}$$

- According sequence $F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$:

$$\wr \frac{x}{2},\, \frac{|x|}{2} \wr \quad \wr 0,\, |x| \wr \quad \wr \frac{x}{2},\, \frac{3|x|}{2} \wr \quad \wr 0,\, 2|x| \wr \quad \cdots \xrightarrow{\omega} \quad \wr 17 \cdot x,\, \infty \cdot |x| \wr$$

Properties of wp Transformer Acting on IWEs

Properties of wp Transformer Acting on IWEs

- **Well–definedness of while–loop semantics:**
  $\lim_{n \to \omega} F^n_{\wr f,\, g \int} \wr 0,\, 0 \int$ always exists and is unique.

Properties of wp Transformer Acting on IWEs

- **Well–definedness of while–loop semantics:**
  $\lim\limits_{n \to \omega} F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$ always exists and is unique.
- **Soundness:**
  If $\mathsf{wp}[C] \wr f,\, |f| \wr = \wr f',\, g' \wr$, $\;g'(\sigma) \neq \infty$,

Properties of wp Transformer Acting on IWEs

- **Well–definedness of while–loop semantics:**
  $\lim\limits_{n \to \omega} F^{n}_{\wr f,\, g \wr} \wr 0,\, 0 \wr$ always exists and is unique.
- **Soundness:**
  If $\mathsf{wp}[C] \wr f,\, |f| \wr = \wr f',\, g' \wr$, $g'(\sigma) \neq \infty$, then

$$f'(\sigma) \;=\; \mathsf{EV}_{[\![C]\!]_\sigma}(f)\;.$$

Properties of wp Transformer Acting on IWEs

- **Well–definedness of while–loop semantics:**
  $\lim\limits_{n\to\omega} F^n_{\wr f,\, g\int} \wr 0,\, 0\int$ always exists and is unique.
- **Soundness:**
  If $\mathsf{wp}[C]\wr f,\, |f|\int = \wr f',\, g'\int,\;\; g'(\sigma) \neq \infty$, then
  $$f'(\sigma) \;=\; \mathsf{EV}_{[\![C]\!]_\sigma}(f)\;.$$
- **Monotonicity:**
  If $\wr f,\, g\int \;\sqsubseteq\; \wr f',\, g'\int$

Properties of wp Transformer Acting on IWEs

- **Well–definedness of while–loop semantics:**
  $\lim\limits_{n \to \omega} F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$ always exists and is unique.
- **Soundness:**
  If $\mathsf{wp}[C]\wr f,\, |f| \wr = \wr f',\, g' \wr$, $g'(\sigma) \neq \infty$, then
  $$f'(\sigma) \;=\; \mathsf{EV}_{[\![C]\!]_\sigma}(f)\;.$$
- **Monotonicity:**
  If $\wr f,\, g \wr \;\sqsubseteq\; \wr f',\, g' \wr$, then $\mathsf{wp}[C]\wr f,\, g \wr \;\sqsubseteq\; \mathsf{wp}[C]\wr f',\, g' \wr$.

Reasoning about While–Loops

Reasoning about While–Loops

Invariant Rule for While–Loops

Let $I, G \in \mathbb{E}$ and $\{H_n\}_{n \in \mathbb{N}} \subseteq \mathbb{E}$. If

$$F_{|f|+f}(I) \leq I, \quad F_g(G) \leq G,$$
$$H_0 \leq F_{|f|}(0), \quad \text{and} \quad H_{n+1} \leq F_{|f|}(H_n),$$

then

$$\mathsf{wp}[\mathtt{while}\,(\xi)\,\{C'\}]\wr f,\, g \wr \;\sqsubseteq\; \Big\wr\, I - \sup_n H_n,\; 2 \cdot G \,\Big\wr\,.$$

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\texttt{:}\quad \texttt{while}\,(1/2)\,\{x \texttt{ := } -x - \mathsf{sign}(x)\}$$

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\texttt{:}\quad \texttt{while}\,(1/2)\,\{x \texttt{ := } -x - \mathsf{sign}(x)\}$$

- Expected value of x after execution of C_{altgeo} is $\dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9}$

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\textbf{:} \quad \texttt{while}\,(1/2)\,\{x \mathrel{\texttt{:=}} -x - \mathsf{sign}(x)\}$$

- Expected value of x after execution of C_{altgeo} is $\dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9}$
- Our technique yields $\left\wr \dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9},\ |x| + 1 \right\int$

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\textbf{:} \quad \texttt{while}\,(1/2)\,\{x \texttt{ := } -x - \mathsf{sign}(x)\}$$

- Expected value of x after execution of C_{altgeo} is $\dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9}$
- Our technique yields $\left\langle \dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9},\ |x| + 1 \right\rangle$
- Traditional wp does not allow mixed–sign post expectation x

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\texttt{:}\quad \texttt{while}\,(1/2)\,\{x \texttt{ := } -x - \mathsf{sign}(x)\}$$

- Expected value of x after execution of C_{altgeo} is $\dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9}$
- Our technique yields $\left\langle \dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9},\ |x| + 1 \right\rangle$
- Traditional wp does not allow mixed–sign post expectation x
  - Workaround: Jordan decomposition of x into ${}^{+}x$ and ${}^{-}x$

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\colon \quad \texttt{while}\,(1/2)\,\{x \mathrel{\texttt{:=}} -x - \mathsf{sign}(x)\}$$

- Expected value of x after execution of C_{altgeo} is $\dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9}$
- Our technique yields $\left\langle\!\!\left\langle \dfrac{x}{3} - \dfrac{\mathsf{sign}(x)}{9},\ |x| + 1 \right\rangle\!\!\right\rangle$
- Traditional wp does not allow mixed–sign post expectation x
  - Workaround: Jordan decomposition of x into ${}^{+}x$ and ${}^{-}x$
  - Takes about twice the effort for C_{altgeo} with standard wp

Example

Geometric distribution with alternating sign:

$$C_{altgeo}\texttt{:} \quad \texttt{while}\,(1/2)\,\{x \texttt{ := } -x - \mathsf{sign}(x)\}$$

- Expected value of x after execution of C_{altgeo} is $\frac{x}{3} - \frac{\mathsf{sign}(x)}{9}$
- Our technique yields $\left\langle \frac{x}{3} - \frac{\mathsf{sign}(x)}{9},\ |x| + 1 \right\rangle$
- Traditional wp does not allow mixed–sign post expectation x
  - Workaround: Jordan decomposition of x into ${}^{+}x$ and ${}^{-}x$
  - Takes (me) about twice the effort for C_{altgeo} with standard wp

Summary

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level
- Future work: Connection to an operational semantics

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level
- Future work: Connection to an operational semantics
- Future work: Come up with nicer proof rules for loops!

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level
- Future work: Connection to an operational semantics
- Future work: Come up with nicer proof rules for loops!
- What could all this be useful for (ie. the *actual* motivation)?

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level
- Future work: Connection to an operational semantics
- Future work: Come up with nicer proof rules for loops!
- What could all this be useful for (ie. the *actual* motivation)?
  - Expected values of signed program variables

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level
- Future work: Connection to an operational semantics
- Future work: Come up with nicer proof rules for loops!
- What could all this be useful for (ie. the *actual* motivation)?
  - Expected values of signed program variables
  - Calculus for amortized expected run–times

Summary

- Our transformer allows for reasoning about mixed–sign expectations at source code level
- Future work: Connection to an operational semantics
- Future work: Come up with nicer proof rules for loops!
- What could all this be useful for (ie. the *actual* motivation)?
  - Expected values of signed program variables
  - Calculus for amortized expected run–times

Thank you for your kind attention!

Backup Slides: Rules for wp Acting on IWEs

Rules for the wp Transformer Acting on $\mathbb{P}/_{\approx}$

$\boldsymbol{C}$	$\textbf{wp}\,[C]\,\wr \boldsymbol{f},\, \boldsymbol{g} \wr$
`skip`	$\wr f,\, g \wr$

Backup Slides: Rules for wp Acting on IWEs

Rules for the wp Transformer Acting on $\mathbb{P}/{\approx}$

$\boldsymbol{C}$	$\textbf{wp}\,[C]\,\wr \boldsymbol{f},\, \boldsymbol{g} \wr$
`skip`	$\wr f,\, g \wr$
x `:=` E	$\wr f\,[x/E]\,,\, g\,[x/E] \wr$

Backup Slides: Rules for wp Acting on IWEs

Rules for the wp Transformer Acting on $\mathbb{P}/_{\approx}$

$\boldsymbol{C}$	$\textbf{wp}\,[C]\,\wr \boldsymbol{f},\, \boldsymbol{g} \int$
`skip`	$\wr f,\, g \int$
x `:=` E	$\wr f\,[x/E]\,,\, g\,[x/E] \int$
$C_1\,;\,C_2$	$\mathsf{wp}\,[C_1]\,(\mathsf{wp}[C_2]\wr f,\, g \int)$

Backup Slides: Rules for wp Acting on IWEs

Rules for the wp Transformer Acting on $\mathbb{P}/\approx$

C	$\mathsf{wp}\,[C]\,\wr f,\, g \int$
`skip`	$\wr f,\, g \int$
x `:=` E	$\wr f\,[x/E]\,,\, g\,[x/E] \int$
C_1 `;` C_2	$\mathsf{wp}\,[C_1]\,(\mathsf{wp}[C_2]\wr f,\, g \int)$
`if` $(\xi)\ \{C_1\}$ `else` $\{C_2\}$	$[\![\xi]\!] \cdot \mathsf{wp}[C_1]\wr f,\, g \int + [\![\neg\xi]\!] \cdot \mathsf{wp}[C_2]\wr f,\, g \int$

Backup Slides: Rules for wp Acting on IWEs

Rules for the wp Transformer Acting on $\mathbb{P}/{\approx}$

$\boldsymbol{C}$	$\textbf{wp}\,[C]\,\wr\boldsymbol{f},\,\boldsymbol{g}\wr$
`skip`	$\wr f,\, g\wr$
x `:=` E	$\wr f\,[x/E]\,,\, g\,[x/E]\wr$
C_1 `;` C_2	$\mathsf{wp}\,[C_1]\,(\mathsf{wp}[C_2]\wr f,\, g\wr)$
`if` $(\xi)\,\{C_1\}$ `else` $\{C_2\}$	$[\![\xi]\!]\cdot\mathsf{wp}[C_1]\wr f,\, g\wr + [\![\neg\xi]\!]\cdot\mathsf{wp}[C_2]\wr f,\, g\wr$
`while` $(\xi)\,\{C'\}$	$\lim\limits_{n\to\omega}\; F^{n}_{\wr f,\, g\wr}\wr 0,\, 0\wr$

$$F_{\wr f,\, g\wr}\wr X,\, Y\wr \;=\; [\![\neg\xi]\!]\cdot\wr f,\, g\wr + [\![\xi]\!]\cdot\mathsf{wp}[C']\wr X,\, Y\wr$$

Backup Slides: Reasoning about While–Loops

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent
- If $\sum a_i$ abs. conv., then $\sum a_i = \sum \big(|a_i| + a_i\big) - \sum |a_i|$

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent
- If $\sum a_i$ abs. conv., then $\sum a_i = \sum \big(|a_i| + a_i\big) - \sum |a_i|$
- Apply this principle to $F_{\wr f,\, g \wr}$:

$$F^n_{\wr f,\, g \wr}\wr 0,\, 0 \wr \;=\; \Big\wr\, F^n_{|f|+f}(0) - F^n_{|f|}(0),\;\; F^n_g(0) \Big\wr$$

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent
- If $\sum a_i$ abs. conv., then $\sum a_i = \sum \big(|a_i| + a_i\big) - \sum |a_i|$
- Apply this principle to $F_{\wr f,\, g \int}$:

$$F^n_{\wr f,\, g \int}\wr 0,\, 0 \int \;=\; \Big\wr\, F^n_{|f|+f}(0) - F^n_{|f|}(0),\;\; F^n_g(0) \Big\int$$

- So how to over–approximate $\lim\limits_{n \to \omega} \;\; F^n_{\wr f,\, g \int}\wr 0,\, 0 \int$ w.r.t. $\sqsubseteq$?

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent
- If $\sum a_i$ abs. conv., then $\sum a_i = \sum \big(|a_i| + a_i\big) - \sum |a_i|$
- Apply this principle to $F_{\wr f,\, g \int}$:

$$F^n_{\wr f,\, g \int}\wr 0,\ 0 \int \;=\; \Big\wr\, F^n_{|f|+f}(0) - F^n_{|f|}(0),\;\; F^n_g(0) \Big\int$$

- So how to over–approximate $\lim\limits_{n \to \omega}\; F^n_{\wr f,\, g \int}\wr 0,\ 0 \int$ w.r.t. $\sqsubseteq$?
  - Over–approximate $\sup\limits_{n} F^n_{|f|+f}(0)$

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent
- If $\sum a_i$ abs. conv., then $\sum a_i = \sum \big(|a_i| + a_i\big) - \sum |a_i|$
- Apply this principle to $F_{\wr f,\, g \int}$:

$$F^n_{\wr f,\, g \int}\wr 0,\, 0 \int \;=\; \Big\wr\, F^n_{|f|+f}(0) - F^n_{|f|}(0),\;\; F^n_{g}(0) \Big\int$$

- So how to over–approximate $\lim\limits_{n \to \omega}\; F^n_{\wr f,\, g \int}\wr 0,\, 0 \int$ w.r.t. $\sqsubseteq$?
  - Over–approximate $\sup\limits_{n} F^n_{|f|+f}(0)$
  - Under–approximate $\sup\limits_{n} F^n_{|f|}(0)$

Backup Slides: Reasoning about While–Loops

- Basic idea: $\sum a_i$ absolutely convergent if $\sum |a_i|$ convergent
- If $\sum a_i$ abs. conv., then $\sum a_i = \sum \big(|a_i| + a_i\big) - \sum |a_i|$
- Apply this principle to $F_{\wr f,\, g \wr}$:

$$F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr \;=\; \Big\wr\, F^n_{|f|+f}(0) - F^n_{|f|}(0),\;\; F^n_g(0) \Big\wr$$

- So how to over–approximate $\lim\limits_{n \to \omega} \; F^n_{\wr f,\, g \wr} \wr 0,\, 0 \wr$ w.r.t. $\sqsubseteq$?
  - Over–approximate $\sup\limits_n F^n_{|f|+f}(0)$
  - Under–approximate $\sup\limits_n F^n_{|f|}(0)$
  - Over–approximate $\sup\limits_n F^n_g(0)$

Backup Slides: Reasoning about While–Loops

Reminder: $F^n_{\wr f,\, g \int}\wr 0,\, 0\int \;=\; \Big\wr F^n_{|f|+f}(0) - F^n_{|f|}(0),\;\; F^n_g(0)\Big\int$

Backup Slides: Reasoning about While–Loops

Reminder: $F^n_{\wr f,\, g \int}\wr 0,\, 0 \int \;=\; \Big\wr F^n_{|f|+f}(0) - F^n_{|f|}(0),\; F^n_g(0) \Big\int$

Invariant Rule for While–Loops

Let $I, G \in \mathbb{E}$ and $\{H_n\}_{n \in \mathbb{N}} \subseteq \mathbb{E}$. If

$$F_{|f|+f}(I) \leq I, \quad F_g(G) \leq G,$$
$$H_0 \leq F_{|f|}(0), \quad \text{and} \quad H_{n+1} \leq F_{|f|}(H_n),$$

then

$$\mathtt{wp}[\mathtt{while}\,(\xi)\,\{C'\}]\wr f,\, g \int \;\sqsubseteq\; \Big\wr I - \sup_n H_n,\; 2 \cdot G \Big\int .$$

Backup Slides: Upper Bounds for wp of While–Loops

Backup Slides: Upper Bounds for wp of While–Loops

Recall the definition of $\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f)$:

$$\mathsf{lfp}\, X \bullet\; [\![\neg\xi]\!] \cdot f + [\![\xi]\!] \cdot \mathsf{wp}\,[C]\,(X)$$

Backup Slides: Upper Bounds for wp of While–Loops

Recall the definition of $\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f)$:

$$\mathsf{lfp}\, X\bullet\ \underbrace{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot \mathsf{wp}\left[C\right](X)}_{=:\ F_f(X)}$$

Backup Slides: Upper Bounds for wp of While–Loops

Recall the definition of $\mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f)$:

$$\mathsf{lfp}\, X\bullet\, \underbrace{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot \mathsf{wp}\,[C]\,(X)}_{=:\ F_f(X)}$$

Theorem: Upper Bounds from Upper Invariants

Let $I \in \mathbb{E}$.

Backup Slides: Upper Bounds for wp of While–Loops

Recall the definition of $\mathsf{wp}\left[\mathtt{while}\left(\xi\right)\left\{C\right\}\right]\left(f\right)$:

$$\mathsf{lfp}\, X\bullet\, \underbrace{[\![\neg\xi]\!] \cdot f + [\![\xi]\!] \cdot \mathsf{wp}\left[C\right]\left(X\right)}_{=:\ F_f(X)}$$

Theorem: Upper Bounds from Upper Invariants

Let $I \in \mathbb{E}$. Then

$$F_f(I) \ \leq\ I$$

Backup Slides: Upper Bounds for wp of While–Loops

Recall the definition of $\mathsf{wp}\,[\mathtt{while}\,(\xi)\,\{C\}]\,(f)$:

$$\mathsf{lfp}\, X\bullet\ \underbrace{[\![\neg\xi]\!]\cdot f + [\![\xi]\!]\cdot \mathsf{wp}\,[C]\,(X)}_{=:\ F_f(X)}$$

Theorem: Upper Bounds from Upper Invariants

Let $I \in \mathbb{E}$. Then

$$F_f(I) \;\leq\; I \quad \text{implies} \quad \mathsf{wp}\,[\mathtt{while}\,(\xi)\,\{C\}]\,(f) \;\leq\; I~.$$

Backup Slides: Lower Bounds for wp of While–Loops

Backup Slides: Lower Bounds for wp of While–Loops

Reasoning on lower bounds is more involved:

Find an argument for being below a least fixed point!

Backup Slides: Lower Bounds for wp of While–Loops

Reasoning on lower bounds is more involved:

Find an argument for being below a least fixed point!

Theorem: Lower Bounds from Lower ω–Invariants

Let $\{I_n\}_{n \in \mathbb{N}} \subseteq \mathbb{E}$.

Backup Slides: Lower Bounds for wp of While–Loops

Reasoning on lower bounds is more involved:

Find an argument for being below a least fixed point!

Theorem: Lower Bounds from Lower ω–Invariants

Let $\{I_n\}_{n\in\mathbb{N}} \subseteq \mathbb{E}$. Then

$$I_0 \;\leq\; F_f(0) \quad \text{and} \quad I_{n+1} \;\leq\; F_f(I_n)$$

Backup Slides: Lower Bounds for wp of While–Loops

Reasoning on lower bounds is more involved:

Find an argument for being below a least fixed point!

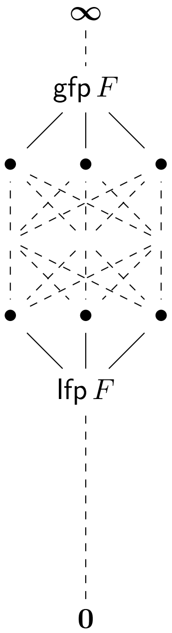
Theorem: Lower Bounds from Lower ω–Invariants

Let $\{I_n\}_{n \in \mathbb{N}} \subseteq \mathbb{E}$. Then

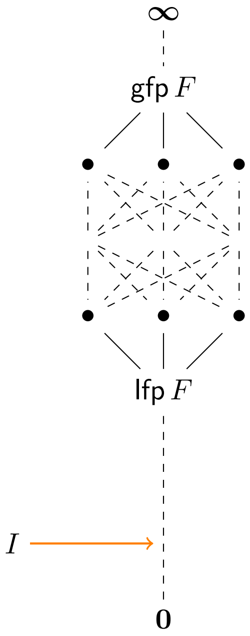
$$I_0 \leq F_f(0) \quad \text{and} \quad I_{n+1} \leq F_f(I_n)$$

$$\text{implies} \quad \sup_{n \in \mathbb{N}} I_n \leq \mathsf{wp}\left[\mathtt{while}\,(\xi)\,\{C\}\right](f) .$$

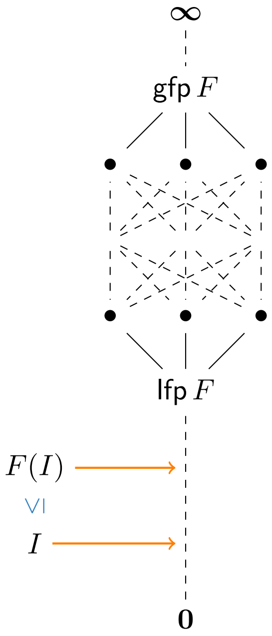
Backup Slides: Park's Lemma



Backup Slides: Park's Lemma

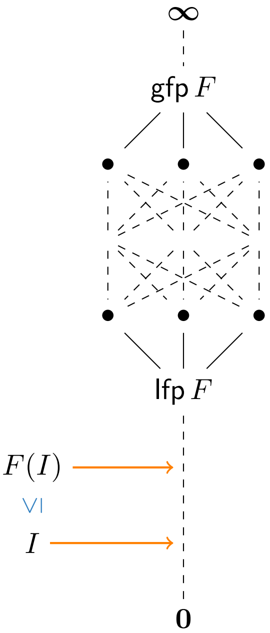


Backup Slides: Park's Lemma



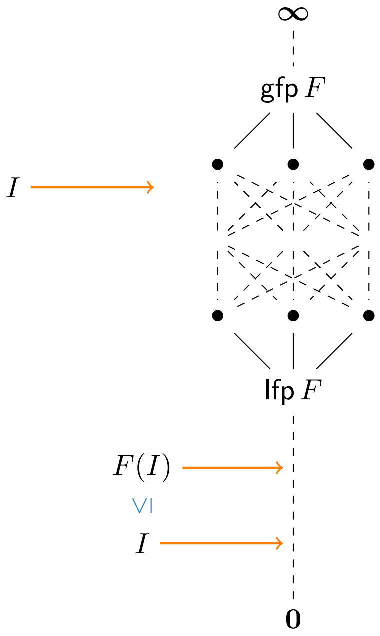
Backup Slides: Park's Lemma

$F(I) \leq I$ implies $\mathsf{lfp}\, F \leq I$



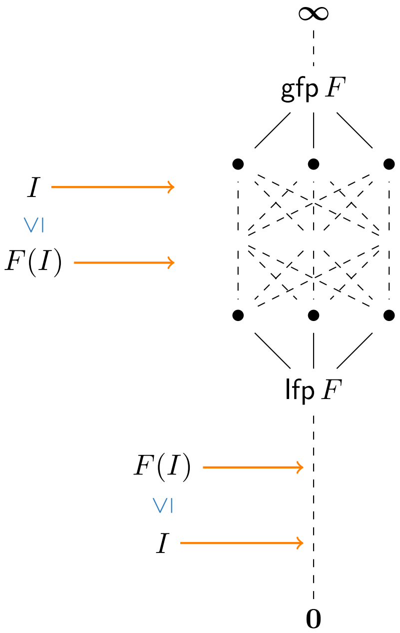
Backup Slides: Park's Lemma

$F(I) \leq I$ implies $\mathsf{lfp}\, F \leq I$



Backup Slides: Park's Lemma

$F(I) \leq I$ implies $\mathrm{lfp}\, F \leq I$



PPDL's While Rule [Kozen '85, p. 168]

$$\neg B \cdot f + B \cdot \langle\, C \,\rangle\, I \;\preceq\; I \quad \text{implies} \quad \langle\, \texttt{while}\,(B)\,\{C\}\,\rangle f \;\preceq\; I\;,$$

for $f \succeq 0$.