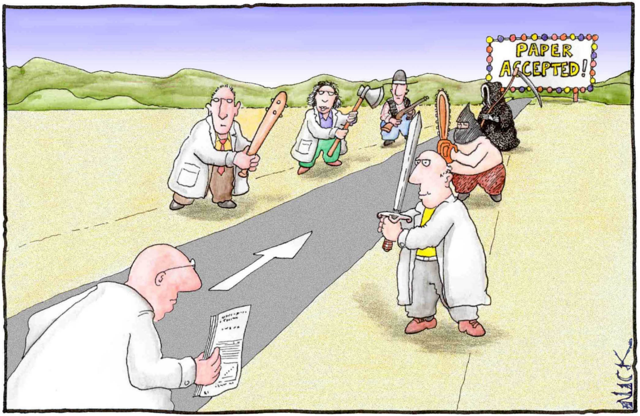
Lower Bounds for Possibly Divergent Probabilistic Programs

Mingshuai Chen

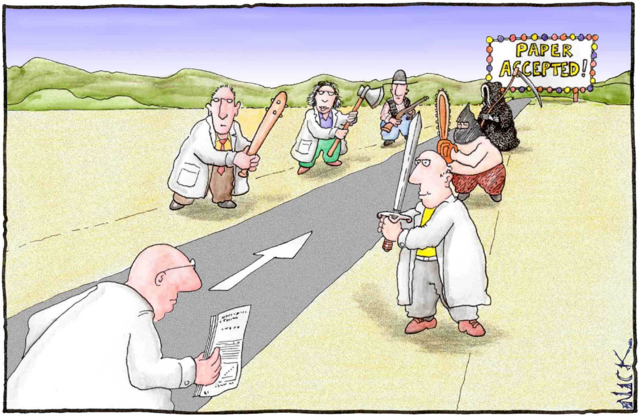
—Joint work with S. Feng, H. Su, B. L. Kaminski, J.-P. Katoen, and N. Zhan—

ROCKS · Nijmegen · May 2022

Work in Progress ...

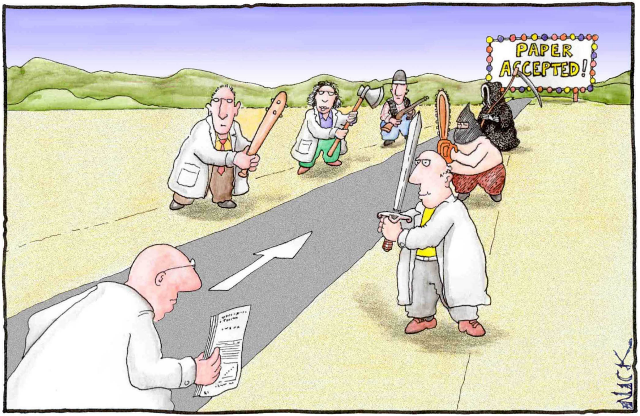


Work in Progress ...



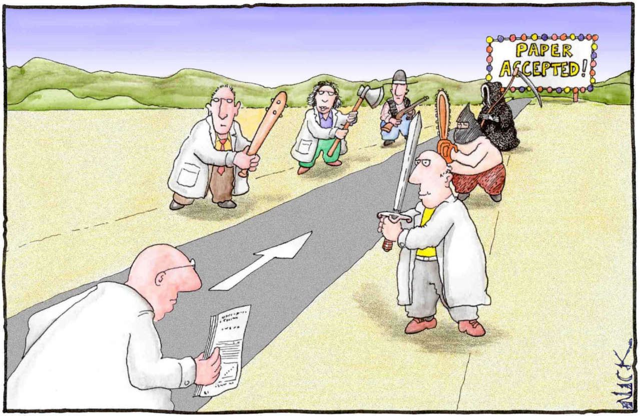
Your Program Diverges? Follow My Rule!

Work in Progress …



M. Hark, B. L. Kaminski, J. Giesl, J.-P. Katoen : **Aiming Low Is Harder** : Induction for Lower Bounds in Probabilistic Program Verification. POPL 2020.

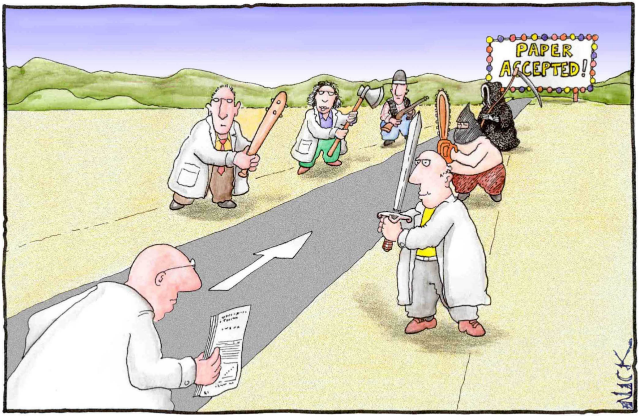
Work in Progress …



Aiming Low Is Not That Hard

M. Hark, B. L. Kaminski, J. Giesl, J.-P. Katoen : **Aiming Low Is Harder** : Induction for Lower Bounds in Probabilistic Program Verification. POPL 2020.

Work in Progress …



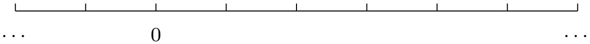
Lower Bounds for Possibly Divergent Probabilistic Programs

Probabilistic Programs

$$C_{\mathsf{brw}}: \quad \texttt{while}\,(\,n > 0\,)\,\{\,n \coloneqq n - 1\;[0.3]\;n \coloneqq n + 1\,\}$$

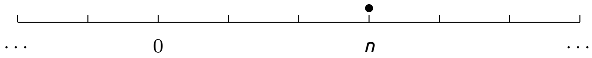
Probabilistic Programs

$$C_{\mathsf{brw}}: \quad \texttt{while}\,(\,n > 0\,)\,\{\,n := n - 1\;[0.3]\;n := n + 1\,\}$$

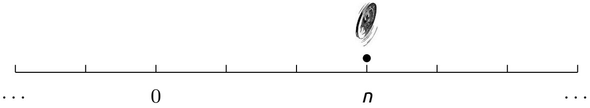


Probabilistic Programs

C_{brw} : $\quad$ `while` $(\, n > 0\,)\,\{\, n := n - 1\; [0.3]\; n := n + 1 \,\}$

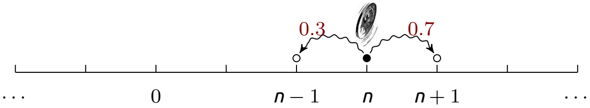


C_{brw} : $\quad$ `while` $(\, n > 0 \,)\,\{\, n \coloneqq n - 1 \;[0.3]\; n \coloneqq n + 1 \,\}$



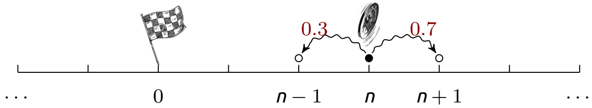
Probabilistic Programs

$$C_{\mathsf{brw}}: \quad \texttt{while}\,(\, n > 0\,)\,\{\, n \coloneqq n - 1\ [0.3]\ n \coloneqq n + 1\,\}$$



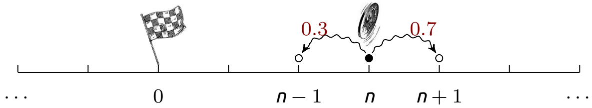
Probabilistic Programs

$$C_{\mathsf{brw}}: \quad \texttt{while}\,(\,n > 0\,)\,\{\, n \coloneqq n - 1 \;[0.3]\; n \coloneqq n + 1 \,\}$$



Probabilistic Programs

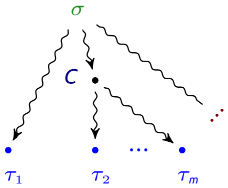
C_{brw} : $\texttt{while}\,(\,n > 0\,)\,\{\,n := n - 1\ [0.3]\ n := n + 1\,\}$

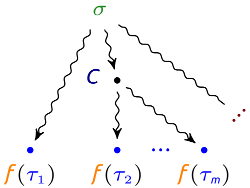


"The crux of probabilistic programming is to treat normal-looking programs as if they were probability distributions."

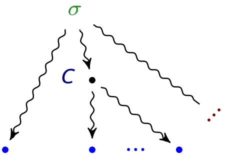
— Michael Hicks, The PL Enthusiast

Quantitative Reasoning about Probabilistic Loops [Kozen; McIver, Morgan; Kaminski]

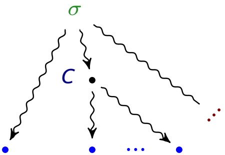



σ
C
$f(\tau_1)$
$f(\tau_2)$
$\cdots$
$f(\tau_m)$

Quantitative Reasoning about Probabilistic Loops [Kozen; McIver, Morgan; Kaminski]



$$\mathsf{wp}[\![C]\!](f)(\sigma) \triangleq \mathsf{Exp}\left[\, f(\tau_1) \quad f(\tau_2) \quad f(\tau_m) \,\right]$$



$$\mathrm{wp}[\![C]\!](f)(\sigma) \triangleq \mathrm{Exp}\Big[\, f(\tau_1) \quad f(\tau_2) \quad \cdots \quad f(\tau_m) \Big]$$

$$\mathrm{wp}[\![\mathtt{while}\,(\,\varphi\,)\,\{\, C \,\}]\!]\,(f) \;=\; \mathrm{lfp}\; \Phi_f \;=\; ?$$

Bounding the Least Fixed Point

$$l \;\preceq\; \mathsf{lfp}\,\Phi_f \;\preceq\; u$$

Bounding the Least Fixed Point

$$l \ \preceq \ \mathsf{lfp}\, \Phi_f \ \preceq \ u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \ \preceq \ u \quad \text{implies} \quad \mathsf{lfp}\, \Phi_f \ \preceq \ u\,.$$

Bounding the Least Fixed Point

$$l \;\preceq\; \mathsf{lfp}\,\Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \;\preceq\; u \quad \text{implies} \quad \mathsf{lfp}\,\Phi_f \;\preceq\; u\,.$$

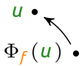
u •

Bounding the Least Fixed Point

$$l \;\preceq\; \mathrm{lfp}\,\Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \;\preceq\; u \quad \text{implies} \quad \mathrm{lfp}\,\Phi_f \;\preceq\; u\,.$$

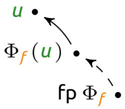


Bounding the Least Fixed Point

$$l \ \preceq\ \mathsf{lfp}\, \Phi_f \ \preceq\ u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \ \preceq\ u \quad \text{implies} \quad \mathsf{lfp}\, \Phi_f \ \preceq\ u\,.$$

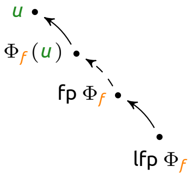


Bounding the Least Fixed Point

$$l \preceq \mathsf{lfp}\ \Phi_f \preceq u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \preceq u \quad \text{implies} \quad \mathsf{lfp}\ \Phi_f \preceq u\,.$$



Bounding the Least Fixed Point

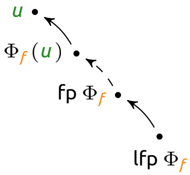
$$\textcolor{blue}{l} \;\preceq\; \mathsf{lfp}\,\Phi_f \;\preceq\; \textcolor{green}{u}$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \preceq u \quad \text{implies} \quad \mathsf{lfp}\,\Phi_f \preceq u\,.$$

- Lower bounds :

$$l \preceq \Phi_f(l) \quad \text{implies} \quad l \preceq \mathsf{lfp}\,\Phi_f\,.$$



Bounding the Least Fixed Point

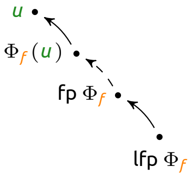
$$l \;\preceq\; \mathsf{lfp}\, \Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \preceq u \quad \text{implies} \quad \mathsf{lfp}\, \Phi_f \preceq u\,.$$

- Lower bounds :

$$l \preceq \Phi_f(l) \quad \text{implies} \quad l \preceq \mathsf{lfp}\, \Phi_f\,.$$



Bounding the Least Fixed Point

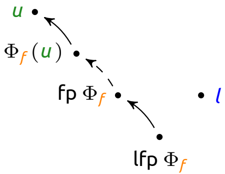
$$l \;\preceq\; \mathrm{lfp}\, \Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

  $\Phi_f(u) \preceq u$ implies $\mathrm{lfp}\, \Phi_f \preceq u$.

- Lower bounds :

  $l \preceq \Phi_f(l)$ ~~implies~~ $l \preceq \mathrm{lfp}\, \Phi_f$.



Bounding the Least Fixed Point

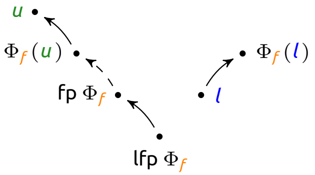
$$l \;\preceq\; \mathsf{lfp}\,\Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \;\preceq\; u \quad \text{implies} \quad \mathsf{lfp}\,\Phi_f \;\preceq\; u\,.$$

- Lower bounds :

$$l \;\preceq\; \Phi_f(l) \quad \cancel{\text{implies}} \quad l \;\preceq\; \mathsf{lfp}\,\Phi_f\,.$$



Bounding the Least Fixed Point

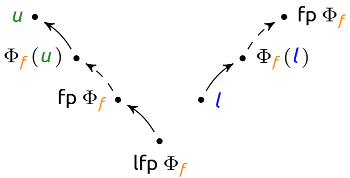
$$l \preceq \operatorname{lfp} \Phi_f \preceq u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \preceq u \quad \text{implies} \quad \operatorname{lfp} \Phi_f \preceq u\,.$$

- Lower bounds :

$$l \preceq \Phi_f(l) \quad \text{~~implies~~} \quad l \preceq \operatorname{lfp} \Phi_f\,.$$



Bounding the Least Fixed Point

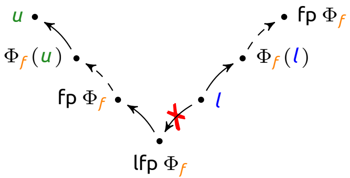
$$l \preceq \mathsf{lfp}\ \Phi_f \preceq u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \preceq u \quad \text{implies} \quad \mathsf{lfp}\ \Phi_f \preceq u\,.$$

- Lower bounds :

$$l \preceq \Phi_f(l) \quad \cancel{\text{implies}} \quad l \preceq \mathsf{lfp}\ \Phi_f\,.$$



Bounding the Least Fixed Point

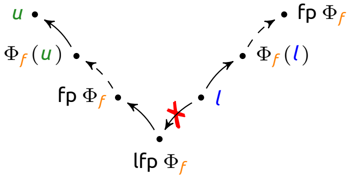
$$l \;\preceq\; \mathsf{lfp}\,\Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \;\preceq\; u \quad \text{implies} \quad \mathsf{lfp}\,\Phi_f \;\preceq\; u\,.$$

- Lower bounds (Hark et al.'s rule) :

$$l \;\preceq\; \Phi_f(l) \;\wedge\; l \text{ is uni. int.} \quad \text{implies} \quad l \;\preceq\; \mathsf{lfp}\,\Phi_f\,.$$



Bounding the Least Fixed Point

$$l \;\preceq\; \mathsf{lfp}\,\Phi_f \;\preceq\; u$$

- Upper bounds (Park induction) :

$$\Phi_f(u) \preceq u \quad \text{implies} \quad \mathsf{lfp}\,\Phi_f \preceq u\,.$$

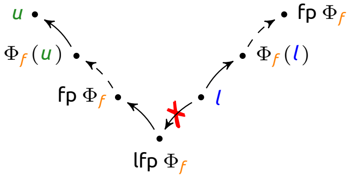
- Lower bounds (Hark et al.'s rule) :

$$l \preceq \Phi_f(l) \;\wedge\; \boxed{l \text{ is uni. int.}} \quad \text{implies} \quad l \preceq \mathsf{lfp}\,\Phi_f\,.$$

almost-sure termination

bounded expectations

...



A New Proof Rule for Lower Bounds

$$\textit{Loop}\colon\quad \texttt{while}\,(\,\varphi\,)\,\{\,C\,\} \quad\rightsquigarrow\quad \textit{Loop}'\colon\quad \texttt{while}\,(\,\varphi'\,)\,\{\,C\,\}$$

A New Proof Rule for Lower Bounds

$$\mathit{Loop}\colon \quad \texttt{while}\,(\,\varphi\,)\,\{\,C\,\} \qquad \rightsquigarrow \qquad \mathit{Loop}'\colon \quad \texttt{while}\,(\,\varphi'\,)\,\{\,C\,\}$$

$$\frac{\varphi' \implies \varphi \qquad l \preceq \mathrm{wp}[\![\mathit{Loop}']\!]\,([\neg\varphi]\cdot f)}{l \preceq \mathrm{wp}[\![\mathit{Loop}]\!]\,(f)}$$

A New Proof Rule for Lower Bounds

$$\mathit{Loop}\colon\quad \texttt{while}\,(\,\varphi\,)\,\{\,C\,\} \quad\rightsquigarrow\quad \mathit{Loop}'\colon\quad \texttt{while}\,(\,\varphi'\,)\,\{\,C\,\}$$

$$\frac{\varphi' \implies \varphi \qquad l \preceq \mathrm{wp}[\![\mathit{Loop}']\!]\,([\neg\varphi]\cdot f)}{l \preceq \mathrm{wp}[\![\mathit{Loop}]\!]\,(f)}$$

- Applicable to *possibly divergent Loop*.

A New Proof Rule for Lower Bounds

$$\mathit{Loop}\colon \quad \texttt{while}\,(\,\varphi\,)\,\{\,C\,\} \qquad \rightsquigarrow \qquad \mathit{Loop}'\colon \quad \texttt{while}\,(\,\varphi'\,)\,\{\,C\,\}$$

$$\frac{\varphi' \implies \varphi \qquad l \preceq \mathrm{wp}[\![\mathit{Loop}']\!]\,([\neg\varphi]\cdot f)}{l \preceq \mathrm{wp}[\![\mathit{Loop}]\!]\,(f)}$$

- Applicable to *possibly divergent Loop*.
- l can be *arbitrarily tight*.

A New Proof Rule for Lower Bounds

$$\mathit{Loop}\colon \quad \texttt{while}\,(\,\varphi\,)\,\{\,C\,\} \qquad \rightsquigarrow \qquad \mathit{Loop}'\colon \quad \texttt{while}\,(\,\varphi'\,)\,\{\,C\,\}$$

$$\frac{\varphi' \implies \varphi \qquad l \preceq \mathrm{wp}[\![\mathit{Loop}']\!]\,([\neg\varphi]\cdot f)}{l \preceq \mathrm{wp}[\![\mathit{Loop}]\!]\,(f)}$$

- Applicable to *possibly divergent Loop*.
- l can be *arbitrarily tight*.
- Reducible to *probabilistic BMC*.

A New Proof Rule for Lower Bounds

$$\mathit{Loop}: \quad \texttt{while}\,(\,\varphi\,)\,\{\,C\,\} \qquad \rightsquigarrow \qquad \mathit{Loop}': \quad \texttt{while}\,(\,\varphi'\,)\,\{\,C\,\}$$

$$\frac{\varphi' \implies \varphi \qquad l \preceq \mathrm{wp}[\![\mathit{Loop}']\!]\,([\neg\varphi]\cdot f)}{l \preceq \mathrm{wp}[\![\mathit{Loop}]\!]\,(f)}$$

- Applicable to *possibly divergent Loop*.
- l can be *arbitrarily tight*.
- Reducible to *probabilistic BMC*.
- Easier to ensure *uni. int.* for Loop'.
- ...

Example : Biased Random Walk

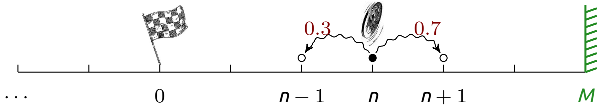
C_{brw} : $\texttt{while}\,(0 < n)\,\{$
$\quad n := n - 1\ [0.3]\ n := n + 1$
$\}$

C_{brw}^{M} : $\texttt{while}\,(0 < n < M)\,\{$
$\quad n := n - 1\ [0.3]\ n := n + 1$
$\}$

Example : Biased Random Walk

C_{brw} : $\quad \texttt{while}\,(0 < n)\,\{$
$\quad\quad n \coloneqq n-1\ [0.3]\ n \coloneqq n+1$
$\quad \}$

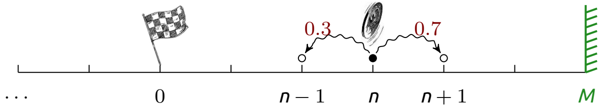
C^{M}_{brw} : $\quad \texttt{while}\,(0 < n < M)\,\{$
$\quad\quad n \coloneqq n-1\ [0.3]\ n \coloneqq n+1$
$\quad \}$



Example : Biased Random Walk

C_{brw}: $\texttt{while}\,(0 < n)\,\{$
$\quad n := n - 1\ [0.3]\ n := n + 1$
$\}$

C_{brw}^{M}: $\texttt{while}\,(0 < n < M)\,\{$
$\quad n := n - 1\ [0.3]\ n := n + 1$
$\}$

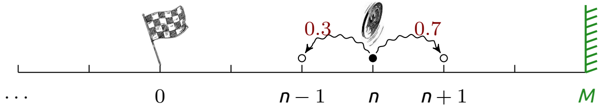


$$l_M(n) \;=\; (3/7)^n - (3/7)^M \,.$$

Example : Biased Random Walk

C_{brw}: $\texttt{while}\,(0 < n)\,\{$
$\quad n \coloneqq n - 1\ [0.3]\ n \coloneqq n + 1$
$\}$

C^{M}_{brw}: $\texttt{while}\,(0 < n < M)\,\{$
$\quad n \coloneqq n - 1\ [0.3]\ n \coloneqq n + 1$
$\}$



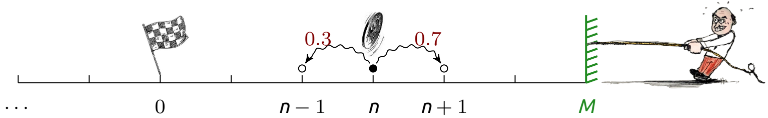
$$l_M(n) \quad = \quad (3/7)^n - (3/7)^M\ .$$

$$\forall M \in \mathbb{N}\colon \quad l_M \ \preceq\ \mathrm{wp}[\![C^{M}_{\text{brw}}]\!]\,([n \leq 0] \cdot 1) \ \preceq\ \mathrm{wp}[\![C_{\text{brw}}]\!]\,(1)\ .$$

Example : Biased Random Walk

C_{brw}: $\texttt{while}\,(0 < n)\,\{$
$\quad n \coloneqq n-1\ [0.3]\ n \coloneqq n+1$
$\}$

C^M_{brw}: $\texttt{while}\,(0 < n < M)\,\{$
$\quad n \coloneqq n-1\ [0.3]\ n \coloneqq n+1$
$\}$



$$l_M(n) \;=\; (3/7)^n - (3/7)^M \;.$$

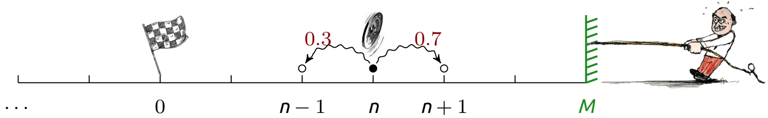
$$\forall M \in \mathbb{N}\colon\quad l_M \;\preceq\; \mathsf{wp}[\![C^M_{\text{brw}}]\!]\,([n \leq 0]\cdot 1) \;\preceq\; \mathsf{wp}[\![C_{\text{brw}}]\!]\,(1)\;.$$

$$(3/7)^n \;=\; \lim_{M\to\infty} l_M \;\preceq\; \mathsf{wp}[\![C_{\text{brw}}]\!]\,(1)\;.$$

Example : Biased Random Walk

C_{brw}: while $(0 < n)$ {
$\quad n := n - 1 \; [0.3] \; n := n + 1$
}

C_{brw}^{M}: while $(0 < n < M)$ {
$\quad n := n - 1 \; [0.3] \; n := n + 1$
}



$$l_M(n) \;=\; (3/7)^n - (3/7)^M \,.$$

$$\forall M \in \mathbb{N}\colon \quad l_M \;\preceq\; \mathsf{wp}[\![C_{\text{brw}}^{M}]\!]\,([n \leq 0] \cdot 1) \;\preceq\; \mathsf{wp}[\![C_{\text{brw}}]\!]\,(1) \,.$$

$$(3/7)^n \;=\; \lim_{M \to \infty} l_M \;\stackrel{\text{Park}}{=}\; \mathsf{wp}[\![C_{\text{brw}}]\!]\,(1) \,.$$