On the Relationship Between Weakest Precondition Transformers and CPS Transformations

Satoshi Kura

20 Dec 2022 @ SYCO 10

National Institute of Informatics
University of Oxford (Visitor)

Program Verification via Hoare Logic

Hoare triple [Hoare, ’69]

precondition $\{P\}\ M\ \{Q\}$ postcondition

Example

$$\{x \geq 0\}\ x \coloneqq x + 1\ \{x \geq 1\}$$

Proof rules

$$\frac{}{\{P\}\ \mathrm{skip}\ \{P\}} \qquad \frac{}{\{P[e/x]\}\ x \coloneqq e\ \{P\}}$$

$$\frac{\{P\}\ M_1\ \{Q\} \qquad \{Q\}\ M_2\ \{R\}}{\{P\}\ M_1; M_2\ \{R\}} \qquad \cdots$$

Weakest Precondition Transformer [Dijkstra, '75]

The **weakest precondition transformer** is a mapping

$$\text{postcondition} \quad \xrightarrow{\mathbf{wp}[M]} \quad \text{precondition}$$

such that

- $\{\mathrm{wp}[M](Q)\}\ M\ \{Q\}$
- $\{P\}\ M\ \{Q\}$ implies $P \implies \mathrm{wp}[M](Q)$.

Then, we have

$$\{P\}\ M\ \{Q\} \qquad \text{iff} \qquad P \implies \mathrm{wp}[M](Q).$$

Calculation of WPTs

To verify $\{P\}\ M\ \{Q\}$,

1. calculate $\mathbf{wp}[M](Q)$
2. check if $P \implies \mathbf{wp}[M](Q)$ holds

If M is an **imperative** program [Dijkstra, '75]:

$$\begin{aligned} \mathbf{wp}[\mathrm{skip}](Q) &= Q \\ \mathbf{wp}[M_1; M_2](Q) &= \mathbf{wp}[M_1](\mathbf{wp}[M_2](Q)) \\ &\vdots \end{aligned}$$

Our Aim

Syntactic calculation of WPTs

for **higher-order effectful programs**

$$\mathbf{wp}[M] = ?$$

Semantics of $\mathbf{wp}[-]$:

generalized for

- various effects
- various properties

[Aguirre & Katsumata, MFPS'20]

Language for M:

- higher order
- algebraic operations

  [Plotkin & Power, FoSSaCS'01]
- recursion

Contributions

Weakest preconditions can be calculated as a **CPS transformation** M^γ:

$$\mathbf{wp}[\llbracket M \rrbracket](Q) = \llbracket M^\gamma\ Q \rrbracket$$

$$\text{program} \quad \xrightarrow{\text{CPS } (-)^\gamma} \quad \text{formula}$$

$\llbracket - \rrbracket$: interpretation

1. **General result** proved using categorical semantics
2. **Two instances** from existing papers

Informal Connection Between CPS and WPT

Given $x : \boldsymbol{\rho} \vdash M : \boldsymbol{\tau}$,

- WPT: $\mathrm{wp}[M] \ : \ (\boldsymbol{\tau} \to \mathbf{Prop}) \to (\boldsymbol{\rho} \to \mathbf{Prop})$
- CPS: $x : \boldsymbol{\rho}^{\gamma} \vdash M^{\gamma} \ : \ (\boldsymbol{\tau}^{\gamma} \to \mathbf{Ans}) \to \mathbf{Ans}$

Informal Connection Between CPS and WPT

Given $x : \rho \vdash M : \tau$,

- WPT: $\mathrm{wp}[M] \ : \ (\tau \to \mathrm{Prop}) \to (\rho \to \mathrm{Prop})$
- CPS: $x : \rho^\gamma \vdash M^\gamma \ : \ (\tau^\gamma \to \mathrm{Ans}) \to \mathrm{Ans}$

If $\rho^\gamma = \rho$, $\tau^\gamma = \tau$, and $\mathrm{Ans} = \mathrm{Prop}$,
by reordering arguments

- CPS: $\lambda Q.\lambda x.M^\gamma\ Q : (\tau \to \mathrm{Prop}) \to (\rho \to \mathrm{Prop})$

Instances

Two instances of the general result:

- Is any output contained in a regular language?

  [Kobayashi et al., ESOP'18]

- Expected cost of randomized programs.

  [Avanzini et al., ICFP'21]

$$\text{Program verification} \xrightarrow[\text{reduction}]{\text{CPS}} \text{Validity of formula}$$

General Result

Setting

Our setting is **parameterised** by parameters for

- syntax
- semantics
- weakest precondition transformer.

We have two languages.

- **Source language** for programs
- **Target language** for logical formulas

$$\text{programs} \quad \xrightarrow{\text{CPS}} \quad \text{formulas}$$

Semantic Weakest Precondition Transformer 1/2

We want **general WPTs**.

- For various **computational effects**
  - Nondeterminism
  - Output
  - Probability
- For expressing **various properties**
  - Any output is in a regular language.
  - Expected cost of randomized programs.

We define WPTs based on [Aguirre & Katsumata, MFPS'20].

Semantic Weakest Precondition Transformer 2/2

Parameter:

EM algebra $\nu : T\Omega \to \Omega$

We define a **WPT** for a program $f : X \to TY$ by

$$\begin{aligned} \mathrm{wp}[f] &: \mathbb{C}(Y, \Omega) \to \mathbb{C}(X, \Omega) \\ \mathrm{wp}[f](Q) &= X \xrightarrow{f} TY \xrightarrow{TQ} T\Omega \xrightarrow{\nu} \Omega \end{aligned}$$

Syntax of Source Language 1/2

We consider the $\boldsymbol{\lambda_c}$-calculus.

Parameter: $\Sigma = (B, K, O)$

- **base type** $b \in B$
  - e.g. $\mathbf{int}$
- **effect-free constant** $\big(c : \mathrm{ar}(c) \to \mathrm{car}(c)\big) \in K$
  - e.g. $(+) : \mathbf{int} \times \mathbf{int} \to \mathbf{int}$
- **algebraic operation** $\big(o : \mathrm{ar}(o) \to \mathrm{car}(o)\big) \in O$
  - e.g. nondeterministic branching $\Box : 1 + 1 \to 1$

Syntax of Source Language 2/2

Type:

$$\rho, \tau \coloneqq b \mid 1 \mid \rho \times \tau \mid 0 \mid \rho + \tau \mid \rho \to \tau \qquad (b \in B)$$

Term:

$$\begin{aligned} M, N \coloneqq{}& x \mid () \mid (M, N) \mid \pi_i M \\ & \mid \delta(M) \mid \iota_i M \mid \delta(M, x_1.N_1, x_2.N_2) \\ & \mid \lambda x.M \mid M\ N \\ & \mid c\ M && \text{effect-free constant } c \in K \\ & \mid o\ M && \text{algebraic operation } o \in O \\ & \mid \mathrm{let\ rec}\ f\ x = M\ \mathrm{in}\ N && \text{recursion} \end{aligned}$$

Semantics of Source Language

Parameter:

$$\mathcal{A} = (\mathbb{C}, T, A, a)$$

- $\mathbb{C}$ (ωCPO-enriched) bicartesian closed **category**
- T (pseudo-lifting) strong **monad** on $\mathbb{C}$
- A, a assign **interpretation** of Σ
  - $Ab \in \mathbb{C}$ for **base type** $b \in B$
  - $a(c)$ for **effect-free constant** $c \in K$
  - $a(o)$ for **algebraic operation** $o \in O$

Interpretation: standard one for λ_c-calculus:

$$\Gamma \vdash M : \rho \qquad \xmapsto{\mathcal{A}[\![-]\!]} \qquad \mathcal{A}[\![M]\!] : \mathcal{A}[\![\Gamma]\!] \to T\mathcal{A}[\![\rho]\!]$$

Syntax of Target Language

Let Ans be an **answer type** (type of **proposition**).

Type:

$$\rho, \tau := \mathrm{Ans} \mid b \mid 1 \mid \rho \times \tau \mid 0 \mid \rho + \tau \mid \rho \to \mathrm{Ans}$$

Term:

$$\begin{aligned} M, N := {} & x \mid () \mid (M, N) \mid \pi_i M \mid \lambda x.M \mid M\ N \\ & \mid \delta(M) \mid \iota_i M \mid \delta(M, x_1.N_1, x_2.N_2) \\ & \mid c\ M && \text{effect-free constant} \\ & \mid o\ M && \text{modal operator} \\ & \mid \mathbf{let\ rec}\ f\ x = M\ \mathbf{in}\ N && \text{fixed point} \end{aligned}$$

Semantics of Target Language

Interpretation:

$$\Gamma \vdash M : \rho \qquad \xmapsto{\mathcal{A}^{\nu}[\![-]\!]} \qquad \mathcal{A}^{\nu}[\![M]\!] : \mathcal{A}^{\nu}[\![\Gamma]\!] \to \mathcal{A}^{\nu}[\![\rho]\!]$$

is the same as **pure STLC** except

- $\mathcal{A}^{\nu}[\![\mathrm{Ans}]\!] = \Omega \qquad =$ (set of truth values)
- $\mathcal{A}^{\nu}[\![o\ M]\!]$ defined using $\nu : T\Omega \to \Omega$

where $\quad \nu : T\Omega \to \Omega$ is an **EM algebra**.

Source Language & Target Language

	Syntax	Semantics
Source	λ_c-calculus	$\mathcal{A}[\![M]\!] : \mathcal{A}[\![\Gamma]\!] \to T\mathcal{A}[\![\rho]\!]$
Target	higher-order logic	$\mathcal{A}^\nu[\![M]\!] : \mathcal{A}^\nu[\![\Gamma]\!] \to \mathcal{A}^\nu[\![\rho]\!]$

Common parameters:

- $\Sigma = (B, K, O)$ for syntax
- $\mathcal{A} = (\mathbb{C}, T, A, a)$ for semantics

CPS Transformation

$$\text{Source language} \quad \xrightarrow[\text{CPS}]{(-)^\gamma} \quad \text{Target language}$$

Based on [Führmann & Thielecke, J.IC'04].

Type:

$$\boldsymbol{\rho} \quad \mapsto \quad \boldsymbol{\rho}^\gamma$$

Context: '

$$\boldsymbol{x_1{:}\rho_1,\ \ldots,\ x_n{:}\rho_n} \quad \mapsto \quad \boldsymbol{x_1{:}\rho_1^\gamma,\ \ldots,\ x_n{:}\rho_n^\gamma}$$

Term:

$$\boldsymbol{\Gamma \vdash M : \rho} \quad \mapsto \quad \boldsymbol{\Gamma^\gamma \vdash M^\gamma : (\rho^\gamma \to \mathrm{Ans}) \to \mathrm{Ans}}$$

Summary of Our Setting

Parameterised by

- $\Sigma = (B, K, O)$ for syntax
- $\mathcal{A} = (\mathbb{C}, T, A, a)$ for semantics
- $\nu : T\Omega \to \Omega$ for weakest precondition transformer.

CPS transformation:

λ_c-calculus $\xrightarrow{(-)^\gamma}$ Higher-order logic

Main Theorem

For any

- well-typed term $\Gamma \vdash M : \rho$
- postcondition $x : \rho \vdash Q : \mathbf{Ans}$

we have

$$\mathrm{wp}[\mathcal{A}[\![M]\!]](\mathcal{A}^{\nu}[\![Q]\!]) \quad = \quad \mathcal{A}^{\nu}[\![M^{\gamma}\ (\lambda x.Q)]\!]$$

if

- types in Γ and ρ do not contain $\to$,
- arity / coarity of $c \in K$ / $o \in O$ do not contain $\to$,
- coarity of $c \in K$ do not contain $0, +$.

CPS as a Syntactic WPT

$$\mathrm{wp}[\mathcal{A}[\![M]\!]](\mathcal{A}^\nu[\![Q]\!]) = \mathcal{A}^\nu[\![M^\gamma\ (\lambda x.Q)]\!]$$

$$\begin{tikzcd}
 & \text{Program} & & \text{Logic} \\
\text{Syntax} & M \arrow[rr, mapsto, "\text{CPS } (-)^\gamma"] \arrow[d, mapsto, "\mathcal{A}[\![-]\!]"] & & M^\gamma \arrow[d, mapsto, "\mathcal{A}^\nu[\![-]\!]"'] \\
\text{Semantics} & \mathcal{A}[\![M]\!] \arrow[r, mapsto, "\text{WPT}"'] & \mathrm{wp}[\mathcal{A}[\![M]\!]] \approx & \mathcal{A}^\nu[\![M^\gamma]\!]
\end{tikzcd}$$

↕ [Aguirre & Katsumata, MFPS’20]

EM algebra

$$\nu : T\Omega \to \Omega$$

Instances

Two instances

Problem	Trace property [Kobayashi et al.]	Expected cost [Avanzini et al.]
Category	$\omega\mathbf{CPO}$	$\omega\mathbf{QBS}$
Algebraic effects	Nondet. & Output	Prob. & Cost
Truth values $\mathcal{A}^{\nu}[\![\mathrm{Ans}]\!]$	$\mathbf{2}^{U}$ (U: states)	$[0, \infty]$

Program verification $\xrightarrow[\text{reduction}]{\text{CPS}}$ Validity of formulas

Instance 1: Trace Property

Is any output string in a regular language?

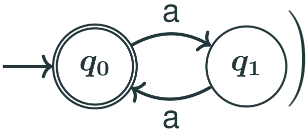
[Kobayashi et al., ESOP'18]

$$\mathrm{Trace}(M) \overset{?}{\subseteq} L(\mathfrak{A})$$

Example:

```
let rec f x = () □ write("aa"); f () in f ()
```

$$\mathrm{Trace}(\texttt{f ()}) = (aa)^* \quad \overset{?}{\subseteq} \quad L\Big(\quad \Big)$$



we don't know this in general

Parameters for Instance 1: Syntax

$$\Sigma = (B, K, O)$$

where O contains

- unary **output** operation

$$\mathbf{event}_a \quad : \quad 1 \to 1$$

- binary **nondeterministic branching** operation

$$\Box \quad : \quad 1 + 1 \to 1$$

Parameters for Instance 1: Semantics

$$\mathcal{A} = (\omega\mathrm{CPO}, T, A, a)$$

where T is defined by the following algebraic theory.
(I.e. TX is a free algebra.)

$$x \,\square\, x = x \qquad x \,\square\, y = y \,\square\, x$$

$$(x \,\square\, y) \,\square\, z = x \,\square\, (y \,\square\, z) \qquad x \leq x \,\square\, y$$

$$\mathrm{event}_a(x \,\square\, y) = \mathrm{event}_a(x) \,\square\, \mathrm{event}_a(y) \qquad x \geq \bot$$

(Hoare powerdomain + output + bottom)

Parameters for Instance 1: EM Algebra

Given a deterministic automaton $\mathfrak{A} = (U, \delta, q_0, F)$,

we define an EM algebra

$$\nu : T\Omega \to \Omega$$

by

$$\Omega = (2^U, \supseteq) \quad \in \quad \omega\mathbf{CPO}$$

- $\bot^\Omega \coloneqq U$ bottom element w.r.t. $\supseteq$
- $x \,\Box^\Omega\, y \coloneqq x \cap y$ "For **any** output s, $s \in L(\mathfrak{A})$."
- $\mathrm{event}_a^\Omega(x) \coloneqq \{q \in U \mid \exists q' \in x, q \xrightarrow{a} q'\} \quad = \langle a \rangle x$

Instance 1: WPT for Trace Property

Assume $F = U$ for $\mathfrak{A} = (U, \delta, q_0, F)$.

$$\begin{aligned} \mathrm{Trace}(M) \subseteq L(\mathfrak{A}) \quad &\iff \quad q_0 \in \mathrm{wp}[\mathcal{A}[\![M]\!]](U) \\ &\iff \quad q_0 \in \mathcal{A}^{\nu}[\![M^{\gamma}\ (\lambda r.\mathrm{true})]\!] \end{aligned}$$

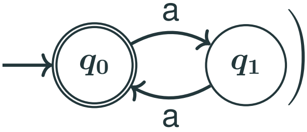
for any $\vdash M : 1$ (so we have $\mathrm{wp}[\mathcal{A}[\![M]\!]] : 2^U \to 2^U$).

Instance 1: Trace Property via CPS

```
let rec f x = () □ write("aa"); f () in f ()
```

The trace property:

$$\mathbf{Trace}(\texttt{f ()}) \quad \subseteq \quad L\Bigg($$



$$\Bigg)$$

is equivalent to

$$q_0 \in \mathcal{A}^{\nu}[\![\text{let rec } f\ x\ k =_{\nu} k\ () \land \langle a\rangle\langle a\rangle(f\ ()\ k) \text{ in}$$
$$f\ ()\ (\lambda r.\text{true})]\!] \quad (\in 2^{U})$$

Two instances

Problem	Trace property [Kobayashi et al.]	Expected cost [Avanzini et al.]
Category	$\omega\mathbf{CPO}$	$\omega\mathbf{QBS}$
Algebraic effects	Nondet. & Output	Prob. & Cost
Truth values $\mathcal{A}^{\nu}[\![\mathrm{Ans}]\!]$	2^{U} (U: states)	$[0, \infty]$

Program verification $\xrightarrow[\text{reduction}]{\text{CPS}}$ Validity of formulas

Instance 2: Expected Cost Analysis

Expected cost of a randomized program

[Avanzini et al., ICFP'21]

$$\mathbf{ect}(M) \quad = \quad ?$$

> **Example**:
>
> $\texttt{let rec f x = () } \oplus_{\boldsymbol{p}} \texttt{ (f ())}^{\checkmark} \texttt{ in f ()}$
>
> $$\mathbf{ect}(\texttt{f ()}) \quad = \quad ?$$

Parameters for Instance 2: Syntax

$$\Sigma = (B, K, O)$$

where O contains

- unary tick operator $(-)^{\checkmark} : 1 \to 1$
  which **increments cost** by 1
- binary **probabilistic branching** $\oplus_p : 1 + 1 \to 1$.

We can add **continuous distributions** too.

- Uniform distribution $\mathbf{unif}_{[0,1]} : \mathbb{R} \to 1$

Parameters for Instance 2: Semantics

$$\boldsymbol{\mathcal{A}} = (\omega\mathbf{QBS},\ \boldsymbol{P}((-)_\perp \times [\mathbf{0}, \boldsymbol{\infty}]),\ \boldsymbol{A},\ \boldsymbol{a})$$

where $\boldsymbol{P}((-)_\perp \times [\mathbf{0}, \boldsymbol{\infty}])$ is the composite of

- **probabilistic powerdomain** monad $\boldsymbol{P}$

  [Vàkàr et al., POPL'19] for $\oplus_p$ and $\mathbf{unif}_{[0,1]}$
- **writer** monad $(-) \times [\mathbf{0}, \boldsymbol{\infty}]$

  for $(-)^{\checkmark}$
- **lifting** monad $(-)_\perp$

  for recursion

Parameters for Instance 2: EM Algebra

We define an EM $P((-)_\perp \times [0,\infty])$-algebra on $[0,\infty]$

$$\nu : P([0,\infty]_\perp \times [0,\infty]) \to [0,\infty]$$

by the composite of

- expectation $\nu^P : P[0,\infty] \to [0,\infty]$
- addition $(+) : [0,\infty] \times [0,\infty] \to [0,\infty]$
- bottom to zero $\nu^{(-)_\perp} : [0,\infty]_\perp \to [0,\infty]$

  s.t. $\nu^{(-)_\perp}(\perp) = 0$

Instance 2: WPT for Expected Cost

$$
\begin{aligned}
\mathbf{ect}(M) &= \mathbf{wp}[\mathcal{A}[\![M]\!]](\boldsymbol{\lambda} r.0) \\
&= \mathcal{A}^{\nu}[\![M^{\gamma}\ (\boldsymbol{\lambda} r.0)]\!]
\end{aligned}
$$

for any $\Gamma \vdash M : \rho$ s.t. Γ, ρ do not contain $\to$

Instance 2: Expected Cost via CPS

$\texttt{let rec f x = ()} \oplus_{\boldsymbol{p}} \texttt{(f ())}^{\checkmark} \texttt{ in f ()}$

$$\mathbf{ect}(\texttt{f ()})$$

$$= \textbf{let rec } \boldsymbol{f}\ \boldsymbol{x}\ \boldsymbol{k} = \boldsymbol{p} \cdot (\boldsymbol{k}\ ()) + (1 - \boldsymbol{p}) \cdot (1 + \boldsymbol{f}\ ()\ \boldsymbol{k}) \textbf{ in}$$

$$\boldsymbol{f}\ ()\ (\boldsymbol{\lambda r}.0)$$

Two instances

Problem	Trace property [Kobayashi et al.]	Expected cost [Avanzini et al.]
Category	$\omega\mathbf{CPO}$	$\omega\mathbf{QBS}$
Algebraic effects	Nondet. & Output	Prob. & Cost
Truth values $\mathcal{A}^{\nu}[\![\mathrm{Ans}]\!]$	$\mathbf{2}^{U}$ (U: states)	$[0, \infty]$

Program verification $\xrightarrow[\text{reduction}]{\text{CPS}}$ Validity of formulas

Conclusion

We proved WPT = CPS

$$\mathbf{wp}[\mathcal{A}[\![M]\!]](\mathcal{A}^{\nu}[\![Q]\!]) = \mathcal{A}^{\nu}[\![M^{\gamma}\ (\lambda x.Q)]\!]$$

parameterised by Σ, $\mathcal{A}$, and ν.

Two instances

- Trace property [Kobayashi et al., ESOP'18]
- Expected cost analysis [Avanzini et al., ICFP'21]

Future Work

- More instances
  - **Conditioning** in probabilistic programs
- Relaxing the last assumption of the main theorem
  - $\mathbf{car}(\boldsymbol{c})$ do not contain $\mathbf{0}, +$ for $\boldsymbol{c} \in \boldsymbol{K}$
- Relationship with **program logics** for higher-order programs

Appendix

Examples of WPTs: Total Correctness

Maybe monad $MX = \{\mathrm{Ok}(x) \mid x \in X\} + \{\mathrm{Fail}\}$

We define $\nu_{\text{total}} : M\Omega \to \Omega$ by

$$\Omega = \{\mathrm{true}, \mathrm{false}\}$$

$$\nu_{\text{total}}(\mathrm{Ok}(x)) = x \qquad \nu_{\text{total}}(\mathrm{Fail}) = \mathrm{false}$$

Then

$$\mathrm{wp}[f](Q) \quad = \quad X \xrightarrow{f} MY \xrightarrow{MQ} M\Omega \xrightarrow{\nu_{\text{total}}} \Omega$$

corresponds to **total correctness**: $\mathrm{wp}[f](Q)(x) = \mathrm{true}$ iff $\exists y \in Y$, $f = \mathrm{Ok}(y)$ and $Q(y) = \mathrm{true}$

Examples of WPTs: Must Modality

Finite nonempty powerset monad PX

We define $\nu_{\text{must}} : P\Omega \to \Omega$ by

$$\Omega = \{\mathrm{true}, \mathrm{false}\}$$

$$\nu_{\text{must}}(\{\mathrm{true}, \mathrm{false}\}) = \mathrm{false}$$

$$\nu_{\text{must}}(\{\mathrm{true}\}) = \mathrm{true} \qquad \nu_{\text{must}}(\{\mathrm{false}\}) = \mathrm{false}$$

Then

$$\mathrm{wp}[f](Q) \quad = \quad X \xrightarrow{f} PY \xrightarrow{PQ} P\Omega \xrightarrow{\nu_{\text{must}}} \Omega$$

corresponds to the **must modality**: $\mathrm{wp}[f](Q)(x) = \mathrm{true}$

iff $\forall y \in f(x), Q(y) = \mathrm{true}$