A Relatively Complete Hoare Logic for Order-Enriched Effects

Sergey Goncharov and Lutz Schröder

October 30, 2012

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Classical Hoare Logic

- **Jundments**: partial correctness assertions: $\{\phi\}\, p\, \{\psi\}$ where
  - ϕ (precondition) and ψ (postcondition) are state-dependent logical assertions;
  - p is a program over the underlying state.
- **Logic**: FOL + (Peano) arithmetic + conventional operations (reading from the memory).
- **Semantics:** $[\![\phi]\!], [\![\psi]\!] : S \to \{0, 1\}$, $[\![p]\!] : S \to S + 1$ where $S = L \to V$ (or $S = L \to V + 1$) is the state.

  Given a state $\sigma \in S$:

$$\sigma \models \{\phi\}\, p\, \{\psi\} \iff (\sigma \models \phi \implies \exists \sigma' = [\![p]\!](\sigma).\ \sigma' \models \psi)$$

Classical Hoare Logic: Some Examples

- $\{x > 1\}\ x := x + 1\ \{x > 2\}$;
- always: $\{\bot\}\ p\ \{\psi\}$ and $\{\phi\}\ p\ \{\top\}$;
- more involved example (factorial):

$$
\begin{array}{l}
\{x = 1; i := 1\} \\
\text{while } (i < n) \text{ do} \\
\qquad i := i + 1; \\
\qquad x := x * i; \\
\{x = n!\}
\end{array}
$$

Classical Hoare Logic: Calculus

(skip) $\dfrac{}{\{\phi\}\ skip\ \{\phi\}}$ **(assign)** $\dfrac{}{\{\phi[a/x]\}\ x := a\ \{\phi\}}$

(seq) $\dfrac{\{\phi\}\ p\ \{\psi\} \quad \{\psi\}\ q\ \{\xi\}}{\{\phi\}\ p; q\ \{\xi\}}$

(if) $\dfrac{\{\phi \wedge b\}\ p\ \{\psi\} \quad \{\phi \wedge \neg b\}\ q\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ p\ \textbf{else}\ q\ \{\psi\}}$

(while) $\dfrac{\{\phi \wedge b\}\ p\ \{\phi\}}{\{\phi\}\ \textbf{while}\ b\ \textbf{do}\ p\ \ \{\phi \wedge \neg b\}}$

(weak) $\dfrac{\phi \Rightarrow \phi' \quad \{\phi'\}\ p\ \{\psi'\} \quad \psi' \Rightarrow \psi}{\{\phi\}\ p\ \{\psi\}}$

Classical Hoare Logic: Properties

- Hoare logic as presented is sound:

$$\Gamma_1, \ldots, \Gamma_n \vdash \Gamma \quad \text{implies} \quad \Gamma_1, \ldots, \Gamma_n \models \Gamma.$$

  Proof: routine verification (boring).

- Hore logic is incomplete (!) for $\models \{\top\}\ p\ \{\bot\}$ iff p does not terminate (non-r.e.).
- Hoare logic is relatively complete or complete in sense of Cook. That is:

$$\models \{\phi\}\ p\ \{\psi\} \quad \text{iff} \quad \Phi \vdash \{\phi\}\ p\ \{\psi\}$$

  where Φ is the set of all valid assertions.

Classical Hoare Logic: Relative Completeness (1/3)

Weakest precondition $\mathsf{wp}(p, \psi)$ is the weakest assertion such that $\{\mathsf{wp}(p, \psi)\}\ p\ \{\psi\}$. Therefore:

$$\{\phi\}\ p\ \{\psi\} \iff (\phi \Rightarrow \mathsf{wp}(p, \psi))$$

Scheme of the proof:

$$\begin{aligned} & \models \{\phi\}\ p\ \{\psi\} \\ \rightsquigarrow\ & \models \phi \Rightarrow \mathsf{wp}(p, \psi) && (1) \\ \rightsquigarrow\ & \Phi \vdash \phi \Rightarrow \mathsf{wp}(p, \psi) && (2) \\ \rightsquigarrow\ & \Phi \vdash \{\phi\}\ p\ \{\psi\} && (3) \end{aligned}$$

This amounts to the properties:

- Existence and uniqness of **wp** (1).
- Expressiveness: sufficient strength of the assertion logic to characterize **wp** (2).
- Provability of $\{\mathsf{wp}(p, \psi)\}\ p\ \{\psi\}$ (3).

Classical Hoare Logic: Relative Completeness (2/3)

Weakest precondition can be defined inductivelly by the clauses:

$$\begin{aligned}
\mathsf{wp}(skip, \psi) &= \psi, \\
\mathsf{wp}(x := a, \psi) &= \psi[a/x], \\
\mathsf{wp}(p; q, \psi) &= \mathsf{wp}(p, \mathsf{wp}(q, \psi)), \\
\mathsf{wp}(\textbf{if } b \textbf{ then } p \textbf{ else } q, \psi) &= (b \Rightarrow \mathsf{wp}(p, \psi)) \wedge (\neg b \Rightarrow \mathsf{wp}(q, \psi)), \\
\mathsf{wp}(\textbf{while } b \textbf{ do } p, \psi) &= \bigwedge_{k \geqslant 0} \xi_k \quad \text{where}
\end{aligned}$$

$\xi_0 = \textbf{true}$ and $\xi_{k+1} = (b \Rightarrow \mathsf{wp}(p, \xi_k)) \wedge (\neg b \Rightarrow \psi)$.

It is provable by induction that this indeed the weakest precondition and $\Phi \vdash \{\mathsf{wp}(p, \psi)\}\ p\ \{\psi\}$.

Note: the same story can be told in terms of strongest postconditions $\mathsf{sp}(p, \phi)$.

Classical Hoare Logic: Gödel's Hack

Note that wp(**while** b **do** p, ψ) as given is not expressible in the language.

Let $\beta(x_1, x_2, x_3) = rem(x + 1, 1 + (x_3 + 1) * x_2)$ (Gödel's β-function).

The β-lemma: for any sequence of natural numbers $k_1, k_1, \ldots, k_n$, there are natural numbers b and c such that, for every $i \leqslant n$, $\beta(b, c, i) = k_i$.

Hence, a statement $\forall k. \forall n_1, \ \ldots, n_k.\ \phi(n_i)$ translates to $\forall k.\ \forall a, b.\ \phi(\beta(b, c, i))$.

Monads Enter

Recall that programs and assertions were interpreted over $S \to S + 1$ and $S \to 2$ correspondingly.

Let $TA = S \to (S \times A) + 1$ (state monad) and $PA = S \to A + 1$ (reader monad).

Then $\Omega_T = P1 = S \to 2$ is a boolean algebra.

More examples:

- $TA = A + E$ (exeptions), $PA = A + 1$, $\Omega_T = 2$;
- $TA = \mathcal{P}(A)$ (non-determinism), $PA = A + 1$, $\Omega_T = 2$;
- $TA = S \to \mathcal{P}(S \times A)$ (states + exeptions), $PA = S \to A + 1$, $\Omega_T = S \to 2$.
- ...

Monads for Generic Programming

Strong monad $\mathbb{T}$: Underlying category $\mathcal{C}$, endofunctor $T : \mathcal{C} \to \mathcal{C}$, unit: $\eta : \mathrm{Id} \to T$ and Kleisli star

$$\_^{\dagger} : \mathrm{hom}(A, TB) \to \mathrm{hom}(TA, TB)$$

plus strength: $\tau_{A,B} : A \times TB \to T(A \times B)$.

Metalanguage of effects:

- $\mathrm{Type}_W ::= W \mid 1 \mid \mathrm{Type}_W \times \mathrm{Type}_W \mid T(\mathrm{Type}_W)$
- Term construction (Cartesian operators omitted):

$$\frac{x : A \in \Gamma}{\Gamma \rhd x : A} \qquad \frac{\Gamma \rhd t : A}{\Gamma \rhd f(t) : B} \quad (f : A \to B \in \Sigma)$$

$$\frac{\Gamma \rhd t : A}{\Gamma \rhd \mathsf{ret}\, t : TA} \qquad \frac{\Gamma \rhd p : TA \quad \Gamma, x : A \rhd q : TB}{\Gamma \rhd \mathsf{do}\ x \leftarrow p; q : TB}$$

Algebraic Operations

Definition: Given $n \in \mathbb{N}$ and a monad $\mathbb{T}$ over $\mathcal{C}$, a natural transformation $\alpha_X : (TX)^n \to TX$ is an (n-ary) algebraic operation if

$$\alpha\langle \mathsf{do}\ x \leftarrow p_i; q\rangle_i = \mathsf{do}\ x \leftarrow \alpha\langle p_i\rangle_i; q$$

Examples include:

- **Exception raising:** one constant $throw : T^0 \to T$.
- **Finite nondeterminism:** one constant $nil : T^0 \to T$ and one operation: $choice : T^2 \to T$. E.g. for $\mathcal{P}$ monad:

  $choice(nil, p) = choice(p, nil) = p.$
- **States:** $lookup_l : T^V \to T$ and $update_{l,v} T \to T$ with $l \in L$, $v \in V$. E.g. for state monad:

  $update_{l,v}(lookup_l\langle p_1, \dots, p_{|V|}\rangle) = update_{l,v}(p_v).$

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

Generic Effects

Under mild assumptions algebraic operations are in one-to-one correspondence with generic effects, i.e. morphisms from $\mathrm{hom}(A, TB)$ [Plotkin and Power, 2001].

Algebraic operations	**Generic effects**
$\mathrm{lookup} : T^V \to T^L$, $\mathrm{update} : T \to T^{L\times V}$	$\mathrm{get} : L \to TV$, $\mathrm{put} : L \times V \to T1$
$\mathrm{nil} : T^0 \to T^1$, $\mathrm{choice} : T^2 \to T$	$\mathrm{nil}_0 : 1 \to T0$, $\mathrm{coin} : 1 \to T2$
$\mathrm{throw} : T^0 \to T^E$	$\mathrm{throw}_0 : E \to T0$

Notably exception handling is not algebraic.

Fixpoint Computations and Order-Enrichment

Let $2 = 1 + 1$, with $\mathcal{C}$ being distributive. We are targeting

$$\textbf{(while)}\quad \frac{\Gamma, x : A \rhd \phi : 2 \qquad \Gamma \rhd p : TA \qquad \Gamma, x : A \rhd q : TA}{\Gamma \rhd \mathsf{init}\; x \leftarrow p \;\mathsf{while}\; \phi \;\mathsf{do}\; q : TA}$$

Definition: A strong monad $\mathbb{T}$ over $\mathcal{C}$ is order-enriched if the following conditions hold.

- Every $\mathrm{hom}(A, TB)$ carries a partial order $\sqsubseteq$, with a bottom $\bot$.
- Every $\mathrm{hom}(A, TB)$ has joins of all directed subsets and has joins of all f, g such that $f \sqsubseteq h$, $g \sqsubseteq h$ for some h.
- For any $h \in \mathrm{hom}(A', A)$ and any $u \in \mathrm{hom}(B \times C, TB')$

  $$f \mapsto f \circ h, \qquad f \mapsto u^{\dagger} \circ f, \qquad f \mapsto \tau\langle \mathrm{id}, f\rangle.$$

  preserve all existing joins (including $\bot$).
- Kleisli star is Scott-continuous, i.e. if $\{f_i \mid i \in I\}$ is a directed subset of $\mathrm{hom}(A, TB)$, then $\bigsqcup_{i \in I} f_i^{\dagger} = (\bigsqcup_{i \in I} f_i)^{\dagger}$.

Fixpoint Computations and Order-Enrichment

Let $2 = 1 + 1$, with $\mathcal{C}$ being distributive. We are targeting

$$\textbf{(while)}\quad \frac{\Gamma, x : A \rhd \phi : 2 \qquad \Gamma \rhd p : TA \qquad \Gamma, x : A \rhd q : TA}{\Gamma \rhd \mathsf{init}\, x \leftarrow p \;\mathsf{while}\; \phi \;\mathsf{do}\; q : TA}$$

Definition: A strong monad $\mathbb{T}$ over $\mathcal{C}$ is order-enriched if the following conditions hold.

- Every $\mathsf{hom}(A, TB)$ carries a partial order $\sqsubseteq$, with a bottom $\bot$.
- Every $\mathsf{hom}(A, TB)$ has joins of all directed subsets and has joins of all f, g such that $f \sqsubseteq h$, $g \sqsubseteq h$ for some h.
- For any $h \in \mathsf{hom}(A', A)$ and any $u \in \mathsf{hom}(B \times C, TB')$

  $$f \mapsto f \circ h, \qquad f \mapsto u^{\dagger} \circ f, \qquad f \mapsto \tau\langle id, f\rangle.$$

  preserve all existing joins (including $\bot$).
- Kleisli star is Scott-continuous, i.e. if $\{f_i \mid i \in I\}$ is a directed subset of $\mathsf{hom}(A, TB)$, then $\bigsqcup_{i \in I} f_i^{\dagger} = \left(\bigsqcup_{i \in I} f_i\right)^{\dagger}$.

Innocence

Definition: Given an order-enriched monad $\mathbb{T}$,

- Two programs p and q commute if
  $\mathsf{do}\ x \leftarrow p; y \leftarrow q; \mathsf{ret}\langle x, y\rangle = \mathsf{do}\ y \leftarrow p; x \leftarrow q; \mathsf{ret}\langle x, y\rangle$
- a program p is copyable w.r.t. $\mathbb{T}$ if
  $\mathsf{do}\ x \leftarrow p; y \leftarrow p; \mathsf{ret}\langle x, y\rangle = \mathsf{do}\ x \leftarrow p; \mathsf{ret}\langle x, x\rangle$;
- a program p is weakly discardable w.r.t. $\mathbb{T}$ if
  $\mathsf{do}\ y \leftarrow p; \mathsf{ret}\,\star \sqsubseteq \mathsf{ret}\,\star$;
- $\mathbb{T}$ is innocent if it is commutative and any program over it is weakly discardable and copyable.

In Nutshell: Innocent monads capture relatively well-behaved computations, but possibly non-terminating.

Innocent Monad for Assertions

Examples:

- Every enriched monad has the partiality monad as the smalles innocent monad.
- The (partial) reader monad $PA = S \to A + 1$ is innocent.

Theorem: Given an innocent monad $\mathbb{P}$,

1. For any two programs $p : P1$ and $q : P1$,

$$p \sqcap q = \mathrm{do}\ \ p; q = \mathrm{do}\ \ q; p.$$

2. The object $P1$ carries a complete Heytling algebra whose underlying distributive lattice structure $(\delta, \upsilon, \epsilon, \rho)$ agrees with the order-enrichment as follows: $\bot_{A,1} = \delta \circ !_A$, $f \sqcup g = \upsilon \circ \langle f, g \rangle$, $\top_{A,1} = \varepsilon \circ !_A$, $f \sqcap g = \rho \circ \langle f, g \rangle$.

A Simple Imperative Metalanguage

$$\textbf{(var)}\ \frac{x : A \in \Gamma}{\Gamma \rhd x : A} \qquad \textbf{(op)}\ \frac{f : A \to B \in \Sigma \qquad \Gamma \rhd t : A}{\Gamma \rhd f(t) : B} \qquad \textbf{(1)}\ \frac{}{\Gamma \rhd \star : 1}$$

$$\textbf{(pair)}\ \frac{\Gamma \rhd t : A \qquad \Gamma \rhd u : B}{\Gamma \rhd \langle t, u \rangle : A \times B} \qquad \textbf{(pr}_1\textbf{)}\ \frac{\Gamma \rhd t : A \times B}{\Gamma \rhd \mathsf{pr}_1\, t : B} \qquad \textbf{(pr}_2\textbf{)}\ \frac{\Gamma \rhd t : A \times B}{\Gamma \rhd \mathsf{pr}_2\, t : B}$$

$$\textbf{(0)}\ \frac{}{\Gamma \rhd 0 : 2} \qquad \textbf{(1)}\ \frac{}{\Gamma \rhd 1 : 2} \qquad \textbf{(if)}\ \frac{\Gamma \rhd b : 2 \qquad \Gamma \rhd s : A \qquad \Gamma \rhd t : A}{\Gamma \rhd \mathsf{if}\ b\ \mathsf{then}\ s\ \mathsf{else}\ t : A}$$

$$\textbf{(do)}\ \frac{\Gamma \rhd p : TA \qquad \Gamma, x : A \rhd q : TB}{\Gamma \rhd \mathsf{do}\ \ x \leftarrow p; q : TB} \qquad \textbf{(ret)}\ \frac{\Gamma \rhd p : A}{\Gamma \rhd \mathsf{ret}\, p : T_{\diamondsuit} A}$$

$$\textbf{(}\diamondsuit\textbf{)}\ \frac{\Gamma \rhd p : T_{\diamondsuit} A}{\Gamma \rhd p : TA} \qquad \textbf{(while)}\ \frac{\Gamma \rhd \phi : 2 \qquad \Gamma \rhd p : TA \qquad \Gamma, x : A \rhd q : TA}{\Gamma \rhd \mathsf{init}\, x \leftarrow p\ \mathsf{while}\ \phi\ \mathsf{do}\ q : TA}$$

Assertions

$$(\top)\;\frac{}{\Gamma \rhd \top : \Omega_\top} \qquad (\wedge)\;\frac{\Gamma \rhd \phi : \Omega_\top \quad \Gamma \rhd \psi : \Omega_\top}{\Gamma \rhd \phi \wedge \psi : \Omega_\top} \qquad (\exists)\;\frac{\Gamma, x : A \rhd \phi : \Omega_\top}{\Gamma \rhd \exists x.\, \phi : \Omega_\top}$$

$$(\bot)\;\frac{}{\Gamma \rhd \bot : \Omega_\top} \qquad (\vee)\;\frac{\Gamma \rhd \phi : \Omega_\top \quad \Gamma \rhd \psi : \Omega_\top}{\Gamma \rhd \phi \vee \psi : \Omega_\top} \qquad (\forall)\;\frac{\Gamma, x : A \rhd \phi : \Omega_\top}{\Gamma \rhd \forall x.\, \phi : \Omega_\top}$$

$$(\Rightarrow)\;\frac{\Gamma \rhd \phi : \Omega_\top \quad \Gamma \rhd \psi : \Omega_\top}{\Gamma \rhd \phi \Rightarrow \psi : \Omega_\top}$$

$$\textbf{(cast)}\;\frac{\Gamma \rhd p : T_\diamond A \quad \Gamma, x : A \rhd \phi : \Omega_\top}{\Gamma \rhd \mathrm{do}\; x \leftarrow p; \phi : \Omega_\top} \qquad \textbf{(pred)}\;\frac{A \to \Omega_\top \in \Gamma}{\Gamma \rhd X : A \to \Omega_\top}$$

$$(\lambda)\;\frac{\Gamma, x : A \rhd t : \Omega_\top}{\Gamma \rhd \lambda x.\; t : A \to \Omega_\top} \qquad \textbf{(app)}\;\frac{\Gamma \rhd t : A \quad \Gamma \rhd s : A \to \Omega_\top}{\Gamma \rhd s(t) : \Omega_\top}$$

$$(\mu)\;\frac{\Gamma, X : A \to \Omega_\top \rhd \phi : A \to \Omega_\top}{\Gamma \rhd \mu X.\, \phi : A \to \Omega_\top} \qquad (\nu)\;\frac{\Gamma, X : A \to \Omega_\top \rhd \phi : A \to \Omega_\top}{\Gamma \rhd \nu X.\, \phi : A \to \Omega_\top}$$

Hoare Logic

We define global judjments $[x \leftarrow p]\,\phi$ by the equivalence:

$$[x \leftarrow p]\,\phi \iff (\mathsf{do}\;\; x \leftarrow p; \phi; \mathsf{ret}\, x) = p.$$

Then let $\{\phi\}x \leftarrow p\{\psi\} = [\phi; x \leftarrow p]\,\psi$.

Some rules:

$$\frac{\{\phi\}\; x \leftarrow p\; \{\psi\} \qquad \{\phi\}\; x \leftarrow p\; \{\chi\}}{\{\phi\}\; x \leftarrow p\; \{\psi \wedge \chi\}} \qquad \frac{\{\psi \wedge \phi?\}\; x \leftarrow p\; \{\chi\} \qquad \{\psi \wedge \neg\phi?\}\; x \leftarrow q\; \{\chi\}}{\{\psi\}\; x \leftarrow (\mathsf{if}\;\phi\;\mathsf{then}\,p\;\mathsf{else}\;q)\; \{\chi\}}$$

$$\frac{\{\phi\}\; y \leftarrow q\; \{\chi\} \qquad \{\psi\}\; y \leftarrow q\; \{\chi\}}{\{\phi \vee \psi\}\; y \leftarrow q\; \{\chi\}} \qquad \frac{\{\psi\}\; x \leftarrow p\; \{\chi\} \qquad \{\chi \wedge \phi?\}\; x \leftarrow q\; \{\chi\}}{\{\psi\}\; x \leftarrow (\mathsf{init}\, x \leftarrow p\;\mathsf{while}\;\phi\;\mathsf{do}\,q)\; \{\chi \wedge \neg\phi\}}$$

Relative Completeness (1/2)

Let us define the weakest precondition:

$$wp(y \leftarrow q, \psi) = \bigsqcup \{\phi \mid \{\phi\}\ y \leftarrow q\ \{\psi\}\}.$$

The desirable properties are:

wp$_1$. $wp(x \leftarrow \mathsf{ret}\, t, \psi) \iff \psi[t/x]$.

wp$_2$. $wp(x \leftarrow f(t), \psi) \iff wp(x \leftarrow f(z), \psi)[t/z]$, with z — any fresh variable

wp$_3$. $wp(x \leftarrow (\mathsf{do}\ \ y \leftarrow p; q), \psi) \iff wp(y \leftarrow p, wp(x \leftarrow q, \psi))$

wp$_4$. $wp(x \leftarrow (\mathsf{if}\ b\ \mathsf{then}\, p\ \mathsf{else}\ q), \psi) \iff$
$(b? \Rightarrow wp(x \leftarrow p, \psi)) \wedge (\bar{b}? \Rightarrow wp(x \leftarrow q, \psi))$

wp$_5$. $wp(x \leftarrow (\mathsf{while}\ b\ \mathsf{do}\, x \leftarrow p), \psi) \iff$
$\nu X.(\lambda x. b? \Rightarrow wp(x \leftarrow p, X(x)) \wedge \bar{b}? \Rightarrow \psi)(x)$

Theorem: If **wp**$_3$ holds (let call it expressiveness) then so do the remaining properties.

Relative Completeness (2/2)

Theorem (Relative Completeness): Let $\mathbb{T}$ be and enriched monad; let $\mathbb{P}$ be an innocent submonad of it. Suppose

1. $\mathbb{P}$ is expressive w.r.t. $\mathbb{T}$;
2. for every $f : A \to TB \in \Sigma_T$ and every assertion ϕ the weakest precondition $wp(x \leftarrow f(y), \psi)$ can be represented by a formula of the assertion language.

Then $\mathbb{T}, \mathbb{P} \models \{\phi\}\ x \leftarrow p\ \{\psi\}$ iff $\Phi \cup \Delta \vdash \{\phi\}\ x \leftarrow p\ \{\psi\}$ where

- Φ is the set of all assertions valid in $\mathbb{P}$;
- Δ is the set of formulas

$$\{wp(x \leftarrow f(y), \psi)\}\ x \leftarrow p\ \{\psi\}.$$

Troubles (1/3)

What exactly expressiveness amounts to?

Let us introduce the strongest postcondition as follows:

$$sp(x, q) = \bigsqcap\{\phi \mid [x \leftarrow q]\,\phi\}.$$

Lemma: Expressiveness is equivalent to any of the following conditions:

a) $[x \leftarrow (\mathrm{do}\ \ y \leftarrow p; q)]\,\psi \implies [y \leftarrow p]\,wp(x \leftarrow q, \psi)$,

b) $[x \leftarrow (\mathrm{do}\ \ y \leftarrow p; q)]\,\psi \implies (sp(y, p) \implies wp(x \leftarrow q, \psi))$,

c) $\{sp(y, p)\}\ x \leftarrow q\ \{sp(x, \mathrm{do}\ \ y \leftarrow p; q)\}$.

Lemma: If the innocent submonad is the partiality monad then expressiveness is equivalent to

$$sp(y, p) \wedge sp(x, q) \implies sp(x, \mathrm{do}\ \ y \leftarrow p; q).$$

Troubles (2/3)

Monads can be given by equational theories: TA — set of terms over variables from A, ret x — variable as term, binding — substitution. E.g. finite powerset:

$$a + (b + c) = (a + b) + c$$

$$a + b = b + a \quad a + a = a + 0 = 0 + a = a$$

Definition: an equational theory is regular if every equation of it has the variables occurring on the left- and right-hand sides.

Lemma: if $\mathbb{T}$ is given by a regular theory partiality monad is expressive w.r.t. it.

Non-example: abelian group monad is non-regular (it has an equation $x - x = 0$) and partiality monad is not expressive w.r.t. it.

Conjecture: partiality monad is expressive w.r.t. $\mathbb{T}$ iff $\mathbb{T}$ is given by a regular theory.

Troubles (3/3)

How to express $wp(x \leftarrow f(y), \phi)$ by a formula?

For the state monad:

- $wp(x \leftarrow \mathrm{get}(l), \phi) = \mathsf{do}\ x \leftarrow \mathrm{get}(l); \phi.$
- In case of static locations: $wp(\mathrm{put}(v, l), \phi) = \phi'$ with ϕ' obtained from ϕ by replacing every $\mathrm{get}(l)$ with $\mathsf{ret}\, v$. Otherwise:

  $wp\big(\mathrm{put}(v, l), \mu X.\lambda x.\big(\mathrm{get}(x) = \mathrm{nil} \vee \mathsf{do}\ x \leftarrow \mathrm{get}(x); X(x)\big)(l)\big) = ?$

More Troubles

Consider the subdistribution monad:

$$TA = \{d : A \to [0,1] \mid \sum_x d(x) \leqslant 1\}$$

It has a parametrised generic effect $\mathtt{coin}_p : T2$. This is not copyable:

$$\begin{aligned}
&\mathsf{do}\ \ x \leftarrow \mathtt{coin}_p; y \leftarrow \mathtt{coin}_p; \mathsf{ret}\langle x, y\rangle \\
&\qquad = [(1,1) \mapsto p * p, (1,2) \mapsto p * (1-p), \\
&\qquad\quad (2,1) \mapsto p * (1-p), (2,2) \mapsto (1-p) * (1-p)] \\
&\mathsf{do}\ \ x \leftarrow \mathtt{coin}_p; \mathsf{ret}\langle x, x\rangle \\
&\qquad = [(1,1) \mapsto p, (2,2) \mapsto (1-p)]
\end{aligned}$$

Hence, the only innocent submonad is the partiality monad. Therefore, e.g. $sp(x, \mathtt{coin}_{1/3}) = (x = 1) \vee (x = 2)$ whereas it had better be something like $x = 1 \oplus_{1/3} x = 2$.

Further Work

- Resolve the troubles.
- Do more case study: local states, quantum computations.
- Come up with a monadic treatment of probabilistic computations.

The End

Thanks for your attention!

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Gordon Plotkin and John Power. Adequacy for algebraic effects. In *Foundations of Software Science and Computation Structures, FoSSaCS 2001*, volume 2030 of *LNCS*, pages 1–24. Springer, 2001.

Gordon Plotkin and John Power. Algebraic operations and generic effects. *Appl. Cat. Struct.*, 11:69–94, 2003.

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG