Observational approach

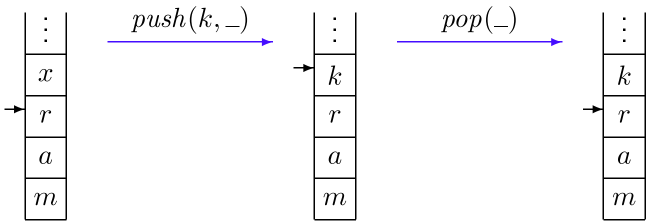
- Observational interpretation of specifications
- Observational refinements
- Observational interpretation of architectural specifications

This is good, but not good enough ...

In basic specifications some axioms are not meant literally:

$$pop(push(e, s)) = s$$

does not hold in some acceptable stack models.



What matters is:

- *observable results* of computations within models

Hence:

- externally observable *behaviour* of models
- internal *indistinguishability* of model elements

To keep things simple:

Let's switch back to the standard algebraic framework.

Assume that all signatures contain sort $bool$ and constants $true$, $false$ interpreted in the standard way in all algebras.

Let's fix for a while a signature $\Sigma = (S, \Omega)$ and a set $OBS \subseteq S$ of *observable sorts*, with $bool \in OBS$.

Observational equivalence

Algebras $A, B \in Alg(\Sigma)$ with $|A|_{OBS} = |B|_{OBS}$ are *observationally equivalent* if they exhibit the same behaviour observable via OBS

- for some X_{OBS} and surjective $v\colon X_{OBS} \to |A|_{OBS} (= |B|_{OBS})$, for each *observable term* $t \in |T_\Sigma(X_{OBS})|_{OBS}$,

$$t_A[v] = t_B[v]$$

Correspondences

- *correspondence* between $A, B \in Alg(\Sigma)$

$$\boxed{\rho\colon A \bowtie B}$$

is a relation $\rho \subseteq |A| \times |B|$ that is *closed under the operations*

- $\rho\colon A \bowtie B$ is *observational* if it is bijective on sorts in OBS

Definition: $A, B \in Alg(\Sigma)$ *are observationally equivalent w.r.t.* OBS

$$\boxed{A \equiv_{OBS} B}$$

if there is an observational correspondence $\rho\colon A \bowtie B$

Observational interpretation of specifications

Given a specification SP with $Sig[SP] = \Sigma = (S, \Omega)$ and $OBS \subseteq S$:

$$Abs_{OBS}[SP] = \{A \in Alg(\Sigma) \mid A \equiv_{OBS} B, \text{ for some } B \in Mod[SP]\}$$

$$\boxed{\textit{For global specifications, choose } OBS = \{bool\}}$$

$$Abs[SP_G] = \{\mathcal{G} \in Alg(\Sigma_G) \mid \mathcal{G} \equiv \mathcal{H}, \text{ for some } \mathcal{H} \in Mod[SP_G]\}$$

An alternative:

Observational indistinguishability

- given $A \in Alg(\Sigma)$, let $\langle A \rangle_{OBS}$ be its subalgebra generated by the observable carriers
- *observational indistinguishability* on A: the largest congruence $\approx_{OBS}$ on $\langle A \rangle_{OBS}$ that is the identity on observable carriers
- *observational quotient* $A/{\approx_{OBS}}$ is the quotient of $\langle A \rangle_{OBS}$ by $\approx_{OBS}$

Fact: *For* $a, b \in |\langle A \rangle_{OBS}|$, $a \approx_{OBS} b$ *if and only if for all observable contexts* $t \in |T_\Sigma(X_{OBS} \cup \{\bullet\})|_{OBS}$ *and valuations* $v\colon X_{OBS} \to |A|_{OBS}$

$$t_A[v[\bullet \mapsto a]] = t_A[v[\bullet \mapsto b]]$$

<u>Assuming some fixed OBS.</u>

Observational satisfaction

- Re-define satisfaction relation:

$$\boxed{A \models_{\approx} \varphi}$$

re-interpreting equality as the indistinguishability.

- Re-interpret specifications:

$$\boxed{Mod_{\approx}[\langle \Sigma, \Phi \rangle] = \{A \in Alg(\Sigma) \mid A \models_{\approx} \varphi, \text{ for all } \varphi \in \Phi\}}$$

Lift this further up to structured specifications (???)

Observational equivalence vs. indistinguishability

Fact: *Factorization property:*

$$A \equiv_{OBS} B \iff A/{\approx_{OBS}} \cong B/{\approx_{OBS}}$$

Fact: *For equational basic specifications*

$$Abs_{OBS}[\langle \Sigma, \Phi \rangle] = Mod_{\approx_{OBS}}[\langle \Sigma, \Phi \rangle]$$

This does not generalize much further!

Observational refinement step

$$\boxed{SP' \overset{\equiv}{\underset{\kappa}{\rightsquigarrow}} SP}$$

Means:

$$\kappa(Mod[SP]) \subseteq Abs[SP']$$

where $\kappa\colon Alg(Sig[SP]) \to Alg(Sig[SP'])$ is a constructor, as before.

Something wrong?

$$\text{NO} \quad \frac{SP'' \overset{\equiv}{\underset{\kappa'}{\rightsquigarrow}} SP' \qquad SP' \overset{\equiv}{\underset{\kappa}{\rightsquigarrow}} SP}{SP'' \overset{\equiv}{\underset{\kappa;\kappa'}{\rightsquigarrow}} SP} \quad \text{NO}$$

Have your cake and eat it too!

- when using a model of a specification, rely on the specification literally
- when building a model for a specification, feel free to do so up to observational equivalence only

Definition: *A constructor $\kappa\colon Alg(\Sigma) \to Alg(\Sigma')$ is stable if it preserves observational equivalence of algebras:*

- *for all $A, B \in Alg(\Sigma)$,*

$$A \equiv B \implies \kappa(A) \equiv \kappa(B)$$

Observational development process

Fact: *Assume all the constructors involved to be stable.*

Then

$$\frac{SP'' \overset{\equiv}{\underset{\kappa'}{\rightsquigarrow}} SP' \qquad SP' \overset{\equiv}{\underset{\kappa}{\rightsquigarrow}} SP}{SP'' \overset{\equiv}{\underset{\kappa;\kappa'}{\rightsquigarrow}} SP}$$

and

$$\frac{SP_0 \overset{\equiv}{\underset{\kappa_1}{\rightsquigarrow}} SP_1 \overset{\equiv}{\underset{\kappa_2}{\rightsquigarrow}} \cdots \overset{\equiv}{\underset{\kappa_n}{\rightsquigarrow}} SP_n = EMPTY}{\kappa_1(\kappa_2(\ldots \kappa_n(empty)\ldots)) \in Abs[SP_0]}$$