A Generic Operational Metathtory for Algebraic Effects

Patricia Johann (Univ. Strathclyde, UK)
Alex Simpson (Univ. Edinburgh, UK)
Janis Voigtländer (Univ. Bonn, Germany)
The operational metatheory of pure functional languages is well established

Our protagonist:

Call-by-name polymorphic PCF

[Plotkin 1977, Pitts 2000]

Small-step (could also give big-step) structural operational semantics:

$$(\lambda x : \tau. M)(N) \rightarrow M[N/x]$$

Ground-type (Nat) contextual equivalence $\equiv_{ctx}$ and preorder $\subseteq_{ctx}$. 
Equational laws:

\[(\lambda x : \tau \ M)(N) =_{ctx} M[N/x]\]
\[(\Lambda \alpha. \ M)[\tau] =_{ctx} M[\tau/\alpha]\] (\beta)

\[\lambda x : \tau. (M x) =_{ctx} M\]
\[\Lambda(M[\alpha]) =_{ctx} M\] (\eta)

Context lemma, cf. [Milner 1977]: \(M \sqsubseteq_{ctx} N : \tau\) if and only if, for every ground-type applicative context \(C[\cdot]\), we have

\[C[M] \rightarrow^* \bar{n} \implies C[N] \rightarrow^* \bar{n}\]

where ground-type applicative contexts are given by:

\[C[\cdot] ::= [\cdot] \mid C[\cdot] M \mid C[\cdot] [\tau]\]

Relational parametricity based on \(\top \top\)-closed relations [Pitts & Stark 1998, Pitts 2000]
What happens if we add effects?
### Structural operational semantics

<table>
<thead>
<tr>
<th>Category</th>
<th>Expression</th>
<th>Transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nondeterminism</td>
<td>$M \lor N$</td>
<td>$M \leftarrow M \lor N \rightarrow N$</td>
</tr>
<tr>
<td>Probabilistic choice</td>
<td>$M \lor N$</td>
<td>$M \lor N \rightarrow \frac{1}{2}M + \frac{1}{2}N$</td>
</tr>
<tr>
<td>Global state</td>
<td>$\text{lookup}_l(\lambda x: \text{Nat. } M)$</td>
<td>$(M, s) \rightarrow (M', s')$</td>
</tr>
<tr>
<td></td>
<td>$\text{update}_l(M; N)$</td>
<td></td>
</tr>
<tr>
<td>Input/output</td>
<td>$\text{read}(\lambda x: \text{Nat. } M)$</td>
<td>$M \xrightarrow{3} M'$</td>
</tr>
<tr>
<td></td>
<td>$\text{write}(M; N)$</td>
<td>$M \xrightarrow{5} M'$</td>
</tr>
</tbody>
</table>
Ground-type preorder

\[ M \sqsubseteq_{basic} N \]

Nondeterminism \hspace{2cm} \text{results}(M) \sqsubseteq_{EM} \text{results}(N)

Probabilistic choice \hspace{2cm} \forall n \in \mathbb{N}. \ P(M \to^* \overline{n}) \leq P(N \to^* \overline{n})

Global state \hspace{2cm} \forall s, n, s'. (M, s) \to^* (\overline{n}, s') \implies (N, s) \to^* (\overline{n}, s')

Input/output \hspace{2cm} \text{io-traces}(M) \subseteq \text{io-traces}(N)

Use \sqsubseteq_{basic} to generate contextual preorder \sqsubseteq_{ctx}
Not terribly surprising (and in some cases known) that:

\[ \beta\eta \]-equational laws + context lemma + \( \top \top \)-closed parametricity
generalise to the effects listed.

Paper provides a **generic operational metatheory** from which these results follow uniformly as instances of general metatheorems.

Talk will focus on

- Uniform formulation of operational semantics + contextual preorder
- Metatheorems and the conditions under which they apply
- Scope and limitations of approach
- Theory of observations
Operational semantics
(cbn version of [Plotkin & Power 2001, Plotkin 2009])

The operational semantics is determined by the signature of effect operations alone.

It is defined as a function mapping closed $M : \tau$ to a computation tree $|M|$, e.g.,

$$|M\overline{1}| = \begin{array}{c}
\text{lookup}_l \\
\text{lookup}_l \\
\text{lookup}_l \\
0 1 2 \cdots \\
\text{lookup}_l \\
\text{lookup}_l \\
\text{lookup}_l \\
0 1 2 \cdots \\
\end{array}
\begin{array}{c}
(\text{update}_l, 1) \\
(\text{update}_l, 2) \\
(\text{update}_l, 3) \\
\cdots \\
\end{array}$$
Contextual preorder

Require a specified basic preorder $\sqsubseteq_{basic}$ on ground-type computation trees.

For example, for global state:

$$t \sqsubseteq_{basic} t' \iff \forall s. \text{exec}(t, s) \downarrow \implies \text{exec}(t, s) = \text{exec}(t', s)$$

Define contextual preorder $\sqsubseteq_{ctx}$ to be the largest typed precongruence which is, at ground type, contained in the basic preorder.

The data determining the operational semantics and contextual preorder is thus:

signature + basic preorder
Generic operational metatheorems

1. Equational laws $\beta\eta$-laws. Contextual equivalences involving effect operations.

2. Ground type completeness For $M, N : \text{Nat}$, we have $M \sqsubseteq_{ctx} N$ iff $|M| \sqsubseteq_{\text{basic}} |N|$.

3. Context lemma $M \sqsubseteq_{ctx} N : \tau$ if and only if, for every ground-type applicative context $C[\cdot]$, we have $|C[M]| \sqsubseteq_{\text{basic}} |C[N]|$.

4. Logical relation Contextual preorder $\sqsubseteq_{ctx}$ is characterised as a $\top\top$-closed logical relation. (This yields a principle of relational parametricity.)

Result 1 holds for any $\sqsubseteq_{\text{basic}}$ (observed by a reviewer)
For results 2–4, we require conditions on $\sqsubseteq_{\text{basic}}$. 
Conditions on $\sqsubseteq_{basic}$

Admissibility
$\sqsubseteq_{basic}$ is admissible if, for all ascending chains $(t_n), (t'_n)$ of ground-type computation trees, if $t_n \sqsubseteq_{basic} t'_n$, for all $n$, then $(\bigcup_{n \geq 0} t_n) \sqsubseteq_{basic} (\bigcup_{n \geq 0} t'_n)$.

Compositional
$\sqsubseteq_{basic}$ is compositional if, whenever $t \sqsubseteq_{basic} t'$ and $t_n \sqsubseteq_{basic} t'_n$, for all $n$, then it holds that $t\{t_n/\overline{n}\}_n \sqsubseteq_{basic} t\{t'_n/\overline{n}\}_n$

Our proofs of 2–4 work for any $\sqsubseteq_{basic}$ that is both admissible and compositional.

For each of the four running examples, $\sqsubseteq_{basic}$ is admissible and compositional.
Scope and limitations

The operational semantics forces the effect operations to be algebraic effects [Plotkin & Power 2001, Plotkin 2009]

By specifying suitable $\sqsubseteq_{basic}$ relations, theory applies to combinations of algebraic effects.

In present framework, only operations of restricted arities (finite or $\text{Nat}$) are allowed. This rules out, e.g., local store, higher-type store, higher-type i/o

Admissibility requirement on $\sqsubseteq_{basic}$ rules out countable nondeterminism

Non-algebraic effects (e.g., control) or effect handlers (e.g., exception handlers) do not fit into framework.
Observational preorder

An observation is a set $O$ of ground-type computation trees.

Frequently $\sqsubseteq_{basic}$ is specified as:

$$t \sqsubseteq_{basic}^{O} t' \iff \forall O \in O. \ t \in O \implies t' \in O$$

where $O$ is a given family of observations.

Our four running examples can all be specified in this way.

E.g., for global state, have observations:

$$s \mapsto (n, s') := \{t \mid \text{exec}(t, s) = (n, s')\}$$
Admissibility

An observation $O$ is Scott-open if, it is up-closed and, for any ascending chain $(t_i)$ with $(\bigcup_i t_i) \in O$, there exists $i$ such that $t_i \in O$.

Proposition  If $O$ is a family of Scott-open observations then $\sqsubseteq^O_{basic}$ is admissible and contains the $\omega$-cpo ordering on trees ($\sqsubseteq$).

Proposition  If $\sqsubseteq_{basic}$ is admissible and contains $\sqsubseteq$ then $\sqsubseteq_{basic}$ arises as $\sqsubseteq^O_{basic}$ for some family Scott-open observations.

In our running examples, the observations determining $\sqsubseteq_{basic}$ are Scott-open.
Compositionality

A family $\mathcal{O}$ of observations is said to be decomposable if whenever $t\{t_n/n\}_n \in O \in \mathcal{O}$, there exist $\mathcal{O}' \subseteq \mathcal{O}$ and $\mathcal{O}'_n \subseteq \mathcal{O}_n$ for all $n$, such that

1. $t \in \bigcap \mathcal{O}'$ and $t_n \in \bigcap \mathcal{O}'_n$, for all $n$
2. for all $t' \in \bigcap \mathcal{O}'$ and $t'_n \in \bigcap \mathcal{O}'_n$, it holds that $t\{t'_n/n\}_n \in O$.

Decomposability says that compositional proof rules of the form

$$
\{x \models O_i\}_{i \in I} \{y_0 \models O_{0,j}\}_{j \in J_0} \{y_1 \models O_{1,j}\}_{j \in J_1} \{y_2 \models O_{2,j}\}_{j \in J_2} \ldots
$$

$$
x\{y_n/n\}_n \models O
$$

are complete for establishing assertions $t\{t_n/n\}_n \models O$
Proposition $\sqsubseteq^{O}_{basic}$ is compositional if and only if $O$ is decomposable. Furthermore, every compositional $\sqsubseteq^{O}_{basic}$ arises as $\sqsubseteq^{O}_{basic}$ for some decomposable family $O$.

In our running examples, the families of observations determining $\sqsubseteq^{O}_{basic}$ are decomposable.

Summary Our running examples are given by decomposable families of Scott-open observations. Hence their basic preorders are admissible and compositional.

Consequence The operational metatheorems apply to the running examples.
Denotationally specified basic preorders
(Not in LICS paper)

[Plotkin 2009] defines contextual preorder using $\omega$-cpo-based denotational semantics to define ground-type preorder.

This idea transfers to our setting, by defining

$$t \sqsubseteq_{\text{basic}} t' \iff [t] \sqsubseteq [t']$$

Such denotationally-defined $\sqsubseteq_{\text{basic}}$ are automatically admissible and compositional.

Our running examples can also be specified in this way.
Future work

- Call-by-value (should be routine)
- Control operators and effect handlers
- Methodical combinations of algebraic effects (perhaps observationally)
- Program logics via observation modalities
- More general arities for operations. E.g., including local store and higher-order store.
- Relaxing admissibility of $\sqsubseteq_{\text{basic}}$, e.g., including countable nondeterminism.