Modal properties of recursively defined commands

Paul Blain Levy, University of Birmingham

A recent paper (“Seeing Beyond Divergence”, W. A. Roscoe, 2004) defines an equivalence relation on programs, and then provides a denotational semantics for this equivalence by using an innovative fixpoint procedure called a reflected fixpoint. Our goal is to distil the essence of this technique, with a view to modelling other equivalence relations such as bisimilarity. The key requirement is to identify when a recursively defined program satisfies a given modal formula A, assuming we already know when programs satisfy the subformulas of A.

For expository purposes we use a very small calculus, but it seems that the results would still be true for a bigger one.

Syntax of Calculus Let A be a set of actions. Our calculus is CCS-like, and has countable nondeterminism and recursion. Its syntax is

\[ M ::= a.M \mid \text{choose}\ \{i.M_i\}_{i\in\mathbb{N}} \mid x \mid \text{rec} \ x.M \]

For any command \( x \vdash M \) we write \( \theta_M \) for the endofunction \( N \mapsto M[N/x] \) on the set of closed terms.

Operational semantics

The relation \( M \Downarrow N \) is defined inductively:

\[
\begin{align*}
\text{choose} \ \{i.M_i\}_{i\in\mathbb{N}} \Downarrow N & \quad & \text{choose} \ \{i.M_i\}_{i\in\mathbb{N}} \Downarrow N \\
\text{rec} \ x.M/N \Downarrow N & \quad & \text{rec} \ x.M/N \Downarrow N \\
a.M \Downarrow M & \quad & M[\text{rec} \ x.M/x] \Downarrow N \\
M_i \Downarrow N & \quad & M[\text{rec} \ x.M/x] \Downarrow N
\end{align*}
\]

The divergence predicate \( M \uparrow \) is defined coinductively:

\[
\text{choose} \ \{i.M_i\}_{i\in\mathbb{N}} \uparrow \quad \text{choose} \ \{i.M_i\}_{i\in\mathbb{N}} \uparrow
\]

\[
\begin{align*}
M_i \uparrow & \quad i \in \text{nat} \\
M[\text{rec} \ x.M/x] \uparrow & \quad \text{rec} \ x.M \uparrow
\end{align*}
\]

Logic We define a modal logic in the style of Hennessy-Milner:

\[
A ::= \neg A \mid \bigvee_{i\in I} A_i \mid \bigwedge_{i\in I} A_i \mid \Diamond a.A \mid \Box \{s.A_s\}_{s\in A^*}
\]

where I is bounded by some suitable cardinal. Informally, \( \Diamond a.A \) means:

It is possible that a will be printed and then A will be satisfied.

And \( \Box \{s.A_s\}_{s\in A^*} \) means:

A time will come when \( A_s \) will be satisfied, where s is the string printed between now and then.

Formally, the satisfaction relation \( M \vDash A \), where M is a closed command, is defined by induction on A:

- Standard clauses for negation, conjunction and disjunction.
- \( M \vDash \Diamond a.A \) when there exists N such that \( M \Downarrow N \) and \( N \vDash A \)
- \( M \vDash \Box \{s.A_s\}_{s\in A^*} \) when

\[
\begin{align*}
\text{choose} \ \{i.M_i\}_{i\in\mathbb{N}} \Downarrow N & \quad \exists k \in \mathbb{N}. (M_k \vDash A_{0a_1\ldots a_{k-1}}) \\
M \Downarrow N & \quad \exists k \leq n. (M_k \vDash A_{0a_1\ldots a_{k-1}})
\end{align*}
\]

Definition 1 Let A be a formula. We define \( \preceq_A \) to be the preorder on closed commands that relates \( M, M' \) when, for any context \( C[\cdot] \), if \( C[M] \vDash A \) then \( C[M'] \vDash A \). We write \( \simeq_A \) for the symmetrization of \( \preceq_A \).

Proposition 1 \( \text{rec} \ x.M \simeq_A M[\text{rec} \ x.M/x] \) for every formula A.

Conjecture 2 Suppose \( C[\text{rec} \ x.M] \vDash B \equiv \Diamond a. A \). Write C for the equivalence class of rec x.M under \( \simeq_A \), so that \( \theta_M \) restricts to an endofunction on C. Then there exists \( n \in \mathbb{N} \) such that, for any \( N \in C \), we have \( C[\theta_M(N)] \vDash B \).

Conjecture 3 Suppose \( C[\text{rec} \ x.M] \vDash B \equiv \Box \{s.A_s\}_{s\in A^*} \). Write C for the equivalence class of rec x.M under the equivalence relation \( \bigcap_{s\in A^*} \simeq_A \), so that \( \theta_M \) restricts to an endofunction on C. There exists an ordinal \( \gamma < \omega_0 \) such that, for any sequence \( (N_n)_{\alpha<\gamma} \) in C satisfying

- \( N_{\alpha+1} = \theta_M(N_{\alpha}) \), for every \( \alpha < \gamma \)
- \( N_{\beta} \) is an upper bound for \( \{N_\alpha \mid \alpha < \beta \} \) in the \( \preceq_B \) preorder, for every limit ordinal \( \beta < \gamma \)

we have \( C[N_\gamma] \vDash B \).