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 $\mathcal{A}$ be a set of actions. Our calculus is CCS-like, and has countable nondeterminism and recursion. Its syntax is

$$M ::= \quad a.M \mid \texttt{choose}\,\{i.M_i\}_{i\in\mathbb{N}} \mid \texttt{x} \mid \texttt{rec x}.\, M$$

For any command $\texttt{x} \vdash M$ we write θ_M for the endofunction $N \mapsto M[N/\texttt{x}]$ on the set of closed terms.

Operational semantics

The relation $M \stackrel{a}{\Rightarrow} N$ is defined inductively:

$$\frac{}{a.M \stackrel{a}{\Rightarrow} M} \qquad \frac{M[\texttt{rec x}.\, M/\texttt{x}] \stackrel{a}{\Rightarrow} N}{\texttt{rec x}.\, M \stackrel{a}{\Rightarrow} N}$$

$$\frac{M_{\hat{\imath}} \stackrel{a}{\Rightarrow} N}{\texttt{choose}\,\{i.M_i\}_{i\in\mathbb{N}} \stackrel{a}{\Rightarrow} N}\ \hat{\imath} \in \texttt{nat}$$

The divergence predicate $M \Uparrow$ is defined coinductively:

$$\frac{M_{\hat{\imath}} \Uparrow}{\texttt{choose}\,\{i.M_i\}_{i\in\mathbb{N}} \Uparrow}\ \hat{\imath} \in \texttt{nat} \qquad \frac{M[\texttt{rec x}.\, M/\texttt{x}] \Uparrow}{\texttt{rec x}.M \Uparrow}$$

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

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

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

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

And $\Box\{s.A_s\}_{s\in\mathcal{A}^*}$ 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 $M \stackrel{a}{\Rightarrow} N$ and $N \vDash A$
- $M \vDash \Box\{s.A_s\}_{s\in\mathcal{A}^*}$ when
  - $M = M_0 \stackrel{a_0}{\Rightarrow} M_1 \stackrel{a_1}{\Rightarrow} \cdots$ implies $\exists k \in \mathbb{N}.\ (M_k \vDash A_{a_0a_1\ldots a_{k-1}})$
  - $M = M_0 \stackrel{a_0}{\Rightarrow} M_1 \stackrel{a_1}{\Rightarrow} \cdots \stackrel{a_{n-1}}{\Rightarrow} M_n \Uparrow$ implies $\exists k \leqslant n.\ (M_k \vDash A_{a_0a_1\ldots a_{k-1}})$

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

Proposition 1 $\texttt{rec x}.\, M \simeq_A M[\texttt{rec x}.\, M/\texttt{x}]$ for every formula A. □

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

Conjecture 3 Suppose $\mathcal{C}[\texttt{rec x}.M] \vDash B \stackrel{\text{def}}{=} \Box\{s.A_s\}_{s\in\mathcal{A}^*}$. Write C for the equivalence class of $\texttt{rec x}.M$ under the equivalence relation $\bigcap_{s\in\mathcal{A}^*} \simeq_{A_s}$, so that θ_M restricts to an endofunction on C. There exists an ordinal $\gamma < \aleph_0$ such that, for any sequence $(N_\alpha)_{\alpha\leqslant\gamma}$ in C satisfying

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

we have $\mathcal{C}[N_\gamma] \vDash B$. □