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

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

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

Operational semantics

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

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

$$\frac{M_{\hat{i}} \overset{\underline{a}}{\Rightarrow} N}{\text{choose } \{i.M_i\}_{i \in \mathbb{N}} \overset{\underline{a}}{\Rightarrow} N} \, \hat{i} \in \mathtt{nat}$$

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

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

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

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

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 $\square \{s.A_s\}_{s \in \mathcal{A}^*}$ 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 $M \models A$, 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 $N \vDash A$
- $M \vDash \square \{s.A_s\}_{s \in \mathcal{A}^*}$ when

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 rec x. $M \simeq_A M[\text{rec x. } M/\text{x}]$ for every formula A. \square

Conjecture 2 Suppose $\mathcal{C}[\operatorname{rec} \mathbf{x}.M] \models B \stackrel{\text{def}}{=} \lozenge a$. A. Write C for the equivalence class of $\operatorname{rec} \mathbf{x}.M$ 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 $\mathcal{C}[\theta_M^n(N)] \models B$. \square

Conjecture 3 Suppose $C[\text{rec } x.M] \models B \stackrel{\text{def}}{=} \Box \{s.A_s\}_{s \in \mathcal{A}^*}$. Write C for the equivalence class of 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
$$C[N_{\gamma}] \models B$$
.