Locally Nameless Representation in Nominal Isabelle

Christian Urban Robert Pollack

Locally nameless representation of terms with binding, using names for free variables, and de Bruijn indices for bound variables, has been used by several researchers for solutions to the POPLmark Challenge. Most of these solutions also use the McKinna–Pollack style, where strengthened induction hypotheses are derived for relations (typing, reduction, ...) by proving equivalence between two versions of the relation. This approach makes the reasoning fairly straightforward, but is very heavy: for every relation one must define an alternative form, and prove equivalence. In this work we show how to considerably lighten the use of this representation using the nominal Isabelle package. The most interesting aspect is that the nominal package can infer a strengthened induction principle for relations, such as typing and reduction, under some simple assumptions.

Consider the following datatype of *locally nameless* pre-terms:

$$t ::= \mathit{Var}\,x \mid \mathit{Bnd}\,i \mid \mathit{App}\,t_1\,t_2 \mid \mathit{Lam}\,t$$

where i is a natural number and x is a variable name. A short-hand for "opening up" a lambda-abstraction is defined as $\mathit{freshen}\,t\,x \stackrel{\text{def}}{=} \mathit{vsub}\ t\ 0\ (\mathit{Var}\,x)$, where the zero-index in t is replaced by the variable x (adjusting the index when moving under a lambda).

Consider now an inductive definition of the simple typing relation:

$$\frac{\mathit{valid}\,\Gamma \quad (x{:}T) \in \Gamma}{\Gamma \vdash_w \mathit{Var}\,x : T}\ \mathit{Var} \qquad \frac{\Gamma \vdash_w t_1 : T_1 \to T_2 \quad \Gamma \vdash_w t_2 : T_2}{\Gamma \vdash_w \mathit{App}\,t_1\,t_2 : T_2}\ \mathit{App}$$

$$\frac{x \,\#\, t \quad (x{:}T_1){::}\Gamma \vdash_w \mathit{freshen}\,t\,x : T_2}{\Gamma \vdash_w \mathit{Lam}\,t : T_1 \to T_2}\ \mathit{Lam}$$

where $x \,\#\, t$ stands for x not occurring in t. It is well known that a simple-minded proof of weakening for this typing relation must use some kind of renaming of variables. In order to avoid doing such renaming arguments over and over in a serious development, McKinna and Pollack introduced an alternative typing relation $\vdash_s$ which is provably equivalent to $\vdash_w$ but gives a stronger induction hypothesis. The proof of equivalence between $\vdash_w$ and $\vdash_s$ packages the renaming once and for all. However establishing the equivalence is not trivial, and also no uniform method for general inductive relations is known.

The main contribution of the work we report here is the observation that $\vdash_w$ meets the requirements so that a strengthened induction principle for $\vdash_w$ can be derived. By supplying some simple facts that verify these requirements, the nominal package can derive the strengthened induction principle automatically and in a uniform way. The principle is strong enough to prove weakening, although apparently not strong enough to prove the equivalence of $\vdash_w$ and $\vdash_s$. More experimentation is required to find the limits of this technique. However, from our experience with the nominal Isabelle package, we conjecture that the reported approach can be used successfully in many rule and structural induction proofs from programming language theory.