Strong Induction Principles in the Locally Nameless Representation of Binders

(Work in Progress)

Christian Urban, TU Munich
Randy Pollack, LFCS Edinburgh

Outline

- “Once upon a time” the contenders in the POPLmark Challenge always made the claim that their approach to binding is the best and all the others are really, really horrible.

  Jeremy Avigad asked me recently “...what was this POPLmark scandal about?”

- Now, general techniques and tools (like Ott) seem to emerge that are independent of the representation of binders.

- I will show that a nominal technique can be used in the locally nameless representation.

  I did/do not know anything about locally nameless representation (Randy, Xavier, Arthur, James, Stephanie. . .).

Strong Induction Principles

- Strong induction principles are designed to (only) deal with the variable convention in proofs.

  Substitution Lemma: If $x \not\equiv y$ and $x \not\in FV(L)$, then
  $$M[x := N][y := L] \equiv M[y := L][x := N[y := L]].$$

  Proving the case $\lambda z.M_1$: "...By the variable convention we may assume that $z \not\equiv x, y$ and z is not free in N, L."

  (nominal_induct M avoiding: x y N L rule: lam.induct)

  Then in the lambda-case one can assume that $z \# (x, y, N, L)$ holds.

- Strong induction principles are used all over the place in nominal verifications.

Strong Rule Inductions

- Strong induction principles derived for structural <u>and</u> rule inductions.

  Weakening Lemma:
  If $\Gamma \vdash t : T$, valid Γ' and $\Gamma \subseteq \Gamma'$, then $\Gamma' \vdash t : T$.

  (nominal_induct Γ t T avoiding: Γ' rule: typing.strong_induct)

  Then in the typing rule for lambdas, one can assume that $x \# \Gamma'$ holds.

- The main point of the strong induction principles: one does not prove the lemma for all binders, but only for some which satisfy additional freshness-constraints (our take on the variable convention).

An Interesting Relation

- As far as I know, in the literature the variable convention concerns binders only.
- Crary, however, describes rules $\Leftrightarrow$ and $\leftrightarrow$ for equivalence-checking:

$$\frac{s \Downarrow p \quad t \Downarrow q \quad \Gamma \vdash p \leftrightarrow q : tbase}{\Gamma \vdash s \Leftrightarrow t : tbase}$$

$$\frac{x \# (\Gamma, s, t) \quad (x, T_1) :: \Gamma \vdash \mathsf{App}\, s\, (\mathsf{Var}\, x) \Leftrightarrow \mathsf{App}\, t\, (\mathsf{Var}\, x) : T_2}{\Gamma \vdash s \Leftrightarrow t : T_1 \to T_2}$$

$$\frac{\mathsf{valid}\, \Gamma \quad (x, T) \in \Gamma}{\Gamma \vdash \mathsf{Var}\, x \leftrightarrow \mathsf{Var}\, x : T}$$

$$\frac{\Gamma \vdash p \leftrightarrow q : T_1 \to T_2 \quad \Gamma \vdash s \Leftrightarrow t : T_1}{\Gamma \vdash \mathsf{App}\, p\, s \leftrightarrow \mathsf{App}\, q\, t : T_2}$$

$$\frac{\mathsf{valid}\, \Gamma}{\Gamma \vdash s \Leftrightarrow t : tunit} \qquad \frac{\mathsf{valid}\, \Gamma}{\Gamma \vdash \mathsf{Const}\, n \leftrightarrow \mathsf{Const}\, n : tbase}$$

An Interesting Relation

- As far as I know, in the literature the variable convention concerns binders only.
- Crary, however, describes rules $\Leftrightarrow$ and $\leftrightarrow$ for equivalence-checking:

$$\frac{s \Downarrow p \quad t \Downarrow q \quad \Gamma \vdash p \leftrightarrow q : tbase}{\Gamma \vdash s \Leftrightarrow t : tbase}$$

$$\frac{x \# (\Gamma, s, t) \quad (x, T_1) :: \Gamma \vdash \mathsf{App}\, s\, (\mathsf{Var}\, x) \Leftrightarrow \mathsf{App}\, t\, (\mathsf{Var}\, x) : T_2}{\Gamma \vdash s \Leftrightarrow t : T_1 \to T_2}$$

$$\frac{\mathsf{valid}\, \Gamma \quad (x, T) \in \Gamma}{\Gamma \vdash \mathsf{Var}\, x \leftrightarrow \mathsf{Var}\, x : T}$$

$$\frac{\Gamma \vdash p \leftrightarrow q : T_1 \to T_2 \quad \Gamma \vdash s \Leftrightarrow t : T_1}{\Gamma \vdash \mathsf{App}\, p\, s \leftrightarrow \mathsf{App}\, q\, t : T_2}$$

$$\frac{\mathsf{valid}\, \Gamma}{\Gamma \vdash s \Leftrightarrow t : tunit} \qquad \frac{\mathsf{valid}\, \Gamma}{\Gamma \vdash \mathsf{Const}\, n \leftrightarrow \mathsf{Const}\, n : tbase}$$

…and proves monotonicity (kind of weakening) in a logical relation proof:

If $\Gamma \vdash s \Leftrightarrow t : T$, valid Γ' and $\Gamma \subseteq \Gamma'$, then $\Gamma' \vdash s \Leftrightarrow t : T$ and
if $\Gamma \vdash s \leftrightarrow t : T$, valid Γ' and $\Gamma \subseteq \Gamma'$, then $\Gamma' \vdash s \leftrightarrow t : T$.

In case of the extensionality rule, one needs the fact that x is fresh for Γ' (otherwise one has to rename).

$$\overline{\Gamma \vdash s \Leftrightarrow t : tbase}$$

$$\frac{x \# (\Gamma, s, t) \quad (x, T_1) :: \Gamma \vdash \mathsf{App}\, s\, (\mathsf{Var}\, x) \Leftrightarrow \mathsf{App}\, t\, (\mathsf{Var}\, x) : T_2}{\Gamma \vdash s \Leftrightarrow t : T_1 \to T_2}$$

$$\frac{\text{valid}\,\Gamma \quad (x, T) \in \Gamma}{\Gamma \vdash \mathsf{Var}\, x \leftrightarrow \mathsf{Var}\, x : T}$$

$$\frac{\Gamma \vdash p \leftrightarrow q : T_1 \to T_2 \quad \Gamma \vdash s \Leftrightarrow t : T_1}{\Gamma \vdash \mathsf{App}\, p\, s \leftrightarrow \mathsf{App}\, q\, t : T_2}$$

$$\frac{\text{valid}\,\Gamma}{\Gamma \vdash s \Leftrightarrow t : tunit} \qquad \frac{\text{valid}\,\Gamma}{\Gamma \vdash \mathsf{Const}\, n \leftrightarrow \mathsf{Const}\, n : tbase}$$

VC-Compatibility

- You can indeed use a variable convention for x in:

$$\frac{x \;\#\; (\Gamma, s, t) \quad (x, T_1) :: \Gamma \vdash \mathsf{App}\, s\, (\mathsf{Var}\, x) \Leftrightarrow \mathsf{App}\, t\, (\mathsf{Var}\, x) : T_2}{\Gamma \vdash s \Leftrightarrow t : T_1 \to T_2}$$

- The reason is that x cannot appear freely in the conclusion of this rule.
- We identified conditions for when the variable convention is safe to use (described later on). These conditions also apply to non-binders.

Locally Nameless

- The lambda-calculus in the locally nameless approach:

$$
\begin{array}{lcl}
\mathit{llam} & = & \mathit{Var}\ \ \mathit{string} \\
 & \mid & \mathit{Bnd}\ \ \mathit{nat} \\
 & \mid & \mathit{App}\ \ \mathit{llam}\ \mathit{llam} \\
 & \mid & \mathit{Lam}\ \ \mathit{llam}
\end{array}
$$

- Has nice properties: e.g. represents alpha-equivalence classes in a canonical way; but needs a well-formed predicate
- ...is a favourite with some people (not really with me, **but this is <u>not</u> the point!!!**)

Typing Relation in LN

- Typing-rules in the locally nameless approach are specified as:

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

$$\frac{x \ \# \ t \quad \{x\!:\!T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \to T_2}$$

$$\frac{}{\mathsf{valid}\ \varnothing} \qquad \frac{x \ \# \ \Gamma \quad \mathsf{valid}\ \Gamma}{\mathsf{valid}\ \{x\!:\!T\} \cup \Gamma}$$

$t\{0 \leftarrow \mathsf{Var}\, x\}$ stands for “replacing” the 0-index with $\mathsf{Var}\, x$

Proof of Weakening

$$\frac{x \# t \quad \{x : T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \to T_2}$$

- If $\Gamma_1 \vdash t : T$ then $\forall \Gamma_2.\ \mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$

- We know:

$\forall \Gamma_2.\ \mathsf{valid}\, \Gamma_2 \wedge \{x : T'\} \cup \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T$

$x \# t$

- We have to show:

$\forall \Gamma_2.\ \mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash \mathsf{Lam}\, t : T' \to T$

Proof of Weakening

$$\frac{x \# t \quad \{x : T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \rightarrow T_2}$$

- If $\Gamma_1 \vdash t : T$ then $\forall \Gamma_2.\, \mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$

- We know:

$\forall \Gamma_2.\, \mathsf{valid}\, \Gamma_2 \wedge \{x : T'\} \cup \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T$

$x \# t$

$\mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2$

- We have to show:

$\Gamma_2 \vdash \mathsf{Lam}\, t : T' \rightarrow T$

Proof of Weakening

$$\frac{x \# t \quad \{x\!:\!T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\,x\} : T_2}{\Gamma \vdash \mathsf{Lam}\,t : T_1 \to T_2}$$

- If $\Gamma_1 \vdash t : T$ then $\forall \Gamma_2.\, \mathsf{valid}\,\Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$

- We know:

$\forall \Gamma_2.\, \mathsf{valid}\,\Gamma_2 \wedge \{x\!:\!T'\} \cup \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t\{0 \leftarrow \mathsf{Var}\,x\} : T$

$x \# t$

$\mathsf{valid}\,\Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2$

- We have to show:

$\Gamma_2 \vdash \mathsf{Lam}\,t : T' \to T$

Proof of Weakening

$$\frac{x \# t \quad \{x : T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \rightarrow T_2}$$

- If $\Gamma_1 \vdash t : T$ then $\forall \Gamma_2.\ \mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$

$$\boxed{\Gamma_2 \mapsto \{x : T'\} \cup \Gamma_2}$$

- We know:

$\forall \Gamma_2.\ \mathsf{valid}\, \Gamma_2 \wedge \{x : T'\} \cup \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T$

$x \# t$

$\mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2$

- We have to show:

$\Gamma_2 \vdash \mathsf{Lam}\, t : T' \rightarrow T$

Proof of Weakening

$$\frac{x \# t \quad \{x\!:\!T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \rightarrow T_2}$$

- If $\Gamma_1 \vdash t : T$ then $\forall \Gamma_2.\, \mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$

$\boxed{\Gamma_2 \mapsto \{x\!:\!T'\} \cup \Gamma_2}$

- We know:

$\forall \Gamma_2.\, \mathsf{valid}\, \Gamma_2 \wedge \{x\!:\!T'\} \cup \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T$

$x \# t$

$\mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \;\Rightarrow\; \{x\!:\!T'\} \cup \Gamma_1 \subseteq \{x\!:\!T'\} \cup \Gamma_2$

- We have to show:

$\Gamma_2 \vdash \mathsf{Lam}\, t : T' \rightarrow T$

Proof of Weakening

$$\frac{x \# t \quad \{x:T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \to T_2}$$

- If $\Gamma_1 \vdash t : T$ then $\forall \Gamma_2.\, \mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$

- We know: $\boxed{\Gamma_2 \mapsto \{x:T'\} \cup \Gamma_2}$

$$\forall \Gamma_2.\, \mathsf{valid}\, \Gamma_2 \wedge \{x:T'\} \cup \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T$$

$x \# t$

$\mathsf{valid}\, \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \;\; \Rightarrow \{x:T'\} \cup \Gamma_1 \subseteq \{x:T'\} \cup \Gamma_2$

valid $\{x:T'\} \cup \Gamma_2$???

- We have to show:

$\Gamma_2 \vdash \mathsf{Lam}\, t : T' \to T$

Existing Solutions

- McKinna-Pollack introduce $\vdash_s$

$$\frac{\forall x.\, x \# \Gamma \Rightarrow \{x : T_1\} \cup \Gamma \vdash_s t\{0 \leftarrow \mathsf{Var}\ x\} : T_2}{\Gamma \vdash_s \mathsf{Lam}\ t : T_1 \rightarrow T_2}$$

They show $\vdash \Leftrightarrow \vdash_s$ and then prove:

If $\Gamma_1 \vdash_s t : T$ then $\forall \Gamma_2.\mathsf{valid}\ \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$.

- Charguéraud et al introduce $\vdash_c$

$$\frac{\forall x \notin L.\, \{x : T_1\} \cup \Gamma \vdash_s t\{0 \leftarrow \mathsf{Var}\ x\} : T_2}{\Gamma \vdash_s \mathsf{Lam}\ t : T_1 \rightarrow T_2}$$

where L is a (finite) list of names

Some Problems:

- It is fair to say that it is still unclear to come up with $\vdash_s$ and $\vdash_c$ in the general case.
- (Related) One likes to be sure to that $\vdash_s$ and $\vdash_c$ are equivalent to $\vdash$. It is annoying to prove this by hand.

If $\Gamma_1 \vdash_s t : T$ then $\forall \Gamma_2.\mathsf{valid}\ \Gamma_2 \wedge \Gamma_1 \subseteq \Gamma_2 \Rightarrow \Gamma_2 \vdash t : T$.

- Charguéraud et al introduce $\vdash_c$

$$\frac{\forall x \notin L.\ \{x : T_1\} \cup \Gamma \vdash_s t\{0 \leftarrow \mathsf{Var}\ x\} : T_2}{\Gamma \vdash_s \mathsf{Lam}\ t : T_1 \rightarrow T_2}$$

where L is a (finite) list of names

Our Approach

- We stay with $\vdash$ and derive a strong induction principle for it (automatically!).
- Conditions that allow us to do this:

  VC-Compatibility:

  - the relation needs to be equivariant, i.e.

    $$\Gamma \vdash t : T \Rightarrow (\pi \bullet \Gamma) \vdash (\pi \bullet t) : (\pi \bullet T)$$

  - what is strengthened must not be in the support of the concl. of the rule

$$\frac{x \# t \quad \{x : T_1\} \cup \Gamma \vdash t\{0 \leftarrow \mathsf{Var}\, x\} : T_2}{\Gamma \vdash \mathsf{Lam}\, t : T_1 \rightarrow T_2}$$

Our Conditions

- What happens when you violate the conditions?

  or, in other words

  Can the variable-convention lead you into trouble?

Our Conditions

- What happens when you violate the conditions?

  or, in other words

  Can the variable-convention lead you into trouble?

  Yes!

$$\frac{}{x \mapsto [\,], x} \qquad \text{bind}\,[\,]\,t = t$$

$$\frac{}{t_1\,t_2 \mapsto [\,], t_1\,t_2} \qquad \text{bind}\,(x :: xs)\,t = \lambda x.(\text{bind}\,xs\,t)$$

$$\frac{t \mapsto xs, t'}{\lambda x.t \mapsto x :: xs, t'}$$

Our Conditions

- Wh
  con
  or,

  You can show:

  If $t \mapsto xs, t'$ then $t =_\alpha \mathsf{bind}\, xs\, t'$.

  Can the variable-convention lead you into trouble?

  Yes!

$$\frac{}{x \mapsto [\,], x} \qquad \mathsf{bind}\, [\,]\, t = t$$

$$\frac{}{t_1\, t_2 \mapsto [\,], t_1\, t_2} \qquad \mathsf{bind}\, (x :: xs)\, t = \lambda x.(\mathsf{bind}\, xs\, t)$$

$$\frac{t \mapsto xs, t'}{\lambda x.t \mapsto x :: xs, t'}$$

A Faulty Lemma

$$\frac{}{x \mapsto [\,], x} \qquad \mathsf{bind}\ [\,]\ t = t$$

$$\frac{}{t_1\, t_2 \mapsto [\,], t_1\, t_2} \qquad \mathsf{bind}\ (x :: xs)\ t = \lambda x.(\mathsf{bind}\ xs\ t)$$

$$\frac{t \mapsto xs, t'}{\lambda x.t \mapsto x :: xs, t'}$$

> If $t \mapsto x :: xs, t'$ and $x \in FV(t')$ then also $x \in FV(\mathsf{bind}\ xs\ t')$.

- The faulty proof: using the variable convention you unbind a term to a list of distinct names
- Two counter-examples

$$\lambda x.\lambda x.x \mapsto [x, x], x$$
$$\lambda y.\lambda z.z \mapsto [y, y], y$$

Some Problems

- The proofs that use the strong induction principles in the nominal approach should also work in the locally nameless approach. For a number of proofs in the "locally nameless wild" the strong induction principles are of no help.
- Knowing that $\vdash \Leftrightarrow \vdash_s \Leftrightarrow \vdash_c$ is still needed in several instances. (There is no infrastructure available that could help you with such proofs.)

Conclusions

- Without modification a nominal technique applied to the locally nameless representation of binders.
- The strong induction principles are derived automatically in N and NL.
- We have conditions for when this possible (unbind is vc-incompatible).
- Bonus: *A* conjecture – the cofinite rules of Charguéraud et al can be derived automatically provided the rules are variable-convention compatible.

Bonus: Strip

- Lo

The relation strip in nominal:

$$\frac{}{x \mapsto x}$$

$$\frac{}{t_1\, t_2 \mapsto t_1\, t_2}$$

$$\frac{t \;\mapsto\; t'}{\lambda x.t \mapsto t'}$$

- The version according to Charguéraud et al

$$\frac{\forall x \notin L.\; t\{0 \leftarrow \mathsf{Var}\, x\} \;\mapsto_c\; t'}{\mathsf{Lam}\, t \mapsto_c t'}$$

Bonus: Strip

- Locally-nameless version:

$$\frac{}{\mathsf{Var}\,x \mapsto \mathsf{Var}\,x}$$

$$\frac{}{\mathsf{App}\,t_1\,t_2 \mapsto \mathsf{App}\,t_1\,t_2}$$

$$\frac{x \# t \quad t\{0 \leftarrow \mathsf{Var}\,x\} \mapsto t'}{\mathsf{Lam}\,t \mapsto t'}$$

- The version according to Charguéraud et al

$$\frac{\forall x \notin L.\ t\{0 \leftarrow \mathsf{Var}\,x\} \mapsto_c t'}{\mathsf{Lam}\,t \mapsto_c t'}$$

Bonus: Strip

- Locally-nameless version:

$$\frac{}{\mathsf{Var}\,x \mapsto \mathsf{Var}\,x}$$

$$\frac{}{\mathsf{App}\,t_1\,t_2 \mapsto \mathsf{App}\,t_1\,t_2}$$

$$\frac{x \# t \quad t\{0 \leftarrow \mathsf{Var}\,x\} \mapsto t'}{\mathsf{Lam}\,t \mapsto t'}$$

- The version according to Charguéraud et al

$$\frac{\forall x \notin L.\ t\{0 \leftarrow \mathsf{Var}\,x\} \mapsto_c t'}{\mathsf{Lam}\,t \mapsto_c t'}$$

$\mathsf{Lam}\,(\mathsf{Bnd}\,0) \mapsto \mathsf{Var}\,x$ but $\mathsf{Lam}\,(\mathsf{Bnd}\,0) \not\mapsto_c \mathsf{Var}\,x$