A Canonical [1] Locally Named Representation of Binding

Randy Pollack
LFCS, University of Edinburgh

Masahiko Sato
Graduate School of Informatics, Kyoto University

Version of September 3, 2009

[1] α-equivalence is identity

Details of This Work

Isabelle theory files:
http://homepages.inf.ed.ac.uk/rpollack/export/SatoPollackSCSS09.tgz

Full paper on previous work (to appear in J. Symbolic Computation):
http://homepages.inf.ed.ac.uk/rpollack/export/SatoPollack09.pdf

Workshop paper on current work:
http://homepages.inf.ed.ac.uk/rpollack/export/SatoPollackSCSS09.pdf

See my web page for these slides and above papers

Outline

Outline

Local Representations

Syntactically distinct classes for (locally) bound variables vs (globally bound) “free” parameters. Different styles:

- Locally named: two species of names; name-carrying abstraction.
  - McKinna/Pollack [TLCA 1993] formalized Pure Type System metatheory.
  - Not canonical representation.
- Locally nameless: names for parameters, de Bruijn indices for locally bound variables.
  - Ademir, Chargueraud, Pierce, Pollack and Weirich [POPL’08].
  - Canonical representation.

This talk: make locally named representation canonical . . .

. . . and do it abstractly.

Why Local Representations?

They are concrete:

- Close to informal usage.
- “Anything true can be proved.”
- Relatively light infrastructure
  (compared to Twelf or nominal Isabelle).
- Can be used in intensional constructive logics (e.g. Coq).

Technically convenient:

- Correct terms are an inductively defined subset of a datatype.
- Constructors (incl. abstraction) are injective.
- Straightforward definitions by primitive recursion.
- Natural inversion principles.

Why Locally Named Representation?

Here I get onto religious ground.

- Locally nameless still has de Bruijn infelicity:
  - Induction hypotheses have to be generalized.
  - Technical issues such as opening an abstraction more complicated.
- Locally named is more beautiful than locally nameless.

Strengthened Induction and Inversion Necessary

- McKinna/Pollack [TLCA'93] [JAR 1999].
- Ademir, Chargueraud, Pierce, Pollack and Weirich [POPL'08]
- Urban and Pollack [WMM'07] *Strong Induction Principles in the Locally Nameless Representation of Binders*.

In this talk I ignore this issue: see above papers

We Will show:

- A canonical, locally named representation . . .
  - . . . refining the representation of McKinna/Pollack (1993) . . .
  - . . . in substitution preserving isomorphism with nominal terms.
- The canonical choice of binding names is interesting and abstract.

Outline

Syntax of pre-terms

Names:

- Countable set $\mathbb{V}$ of atoms used for local *variables*: x, y, z.
- Countable set $\mathbb{X}$ of atoms, used for global *parameters*: X, Y, Z.
    - Only relation needed on $\mathbb{V}$, $\mathbb{X}$ is decidable equality.
    - Nominal Isabelle atom types are convenient.

Symbolic Expressions ($\mathbb{S}$):

- Datatype of pre-terms (pure λ) ranged over by M, N, P, Q:

$$M ::= x \mid X \mid P \cdot Q \mid [x]M$$

    - Usual induction principles for this datatype.
    - Name-carrying syntax.
- In general, may be other classes of variables, parameters and expressions
    - e.g. types and terms in System F.

Occurrences of Names

- Occurrences of global names (parameters)
  - $X \sharp A$ means "*X does not occur syntactically in A*".
    - Easily defined by structural recursion
  - In nominal Isabelle, our $\sharp$ corresponds to nominal freshness (also written $\sharp$).
- Free occurrences of Local Variables (LV)
  - Defined by structural recursion.
  - Respects intended scoping of abstraction.

$$
\begin{aligned}
\mathrm{LV}(X) &\triangleq \{\} \\
\mathrm{LV}(x) &\triangleq \{x\} \\
\mathrm{LV}(M \cdot N) &\triangleq \mathrm{LV}(M) \cup \mathrm{LV}(N) \\
\mathrm{LV}([x]M) &\triangleq \mathrm{LV}(M) - \{x\}
\end{aligned}
$$

Substitution, Concretely

- Concretely defined by *structural* recursion:

$$
\begin{array}{lcl}
[M/X]x & = & x \\
[M/X]Y & = & \text{if } X = Y \text{ then } M \text{ else } Y \\
[M/X]N{\cdot}N & = & ([M/X]N){\cdot}[M/X]N \\
[M/X]([x]N) & = & [x][M/X]N
\end{array}
$$

- Deterministic: no choosing arbitrary names.
  - Thus has natural properties; e.g.

$$
\begin{array}{l}
[X/X]M = M. \\
X \sharp M \implies [P/X]M = M.
\end{array}
$$

- Does not prevent capture, e.g. $[x/X][x]X = [x]x$.
  - Will only be use in safe ways.
- Substitution is a B-algebra homomorophism; see Pollack and Sato (J. Symb. Comp.).

Not Substitution: a purely technical operation

- Used to fill a “hole” (free variable) created by going under a binder.
- Defined by structural recursion:

$$
\begin{array}{lcl}
[M/y]x & = & \text{if } y = x \text{ then } M \text{ else } x \\
[M/y]X & = & X \\
[M/y]([x]N) & = & [x](\text{if } y = x \text{ then } N \text{ else } [M/y]N) \\
[M/y]N_1 \cdot N_2 & = & ([M/y]N_1) \cdot [M/y]N_2
\end{array}
$$

- Respects intended scope of binding.
- Does not prevent capture, e.g. $[x/y][x]y = [x]x$.
- Not a B-algebra homomorophism.

Outline

Overview: Symbolic expressions vs λ-terms

Sexprs do not faithfully represent λ-terms for two reasons.

1. Local variables may appear unbound in sexprs.
    - ‘x’ is an sexpr, but is not intended to represent any λ-term.
        - Remark: ‘X’ is an sexpr representing a λ-term with one (particular) global variable.
    - The fix: select the set of sexprs with no unbound local variables.
        - Call this subset *vclosed* for *variable closed*.
    - Substitution is well-behaved on *vclosed*.
2. Different sexprs in *vclosed* may represent the same λ-term.
    - ‘$[x]x$’ and ‘$[y]y$’; not canonical.
    - The fix: select a canonical subset of *vclosed*.
        - Show that it is an adequate representation of λ-terms.

Overview: Symbolic expressions vs λ-terms

Sexprs do not faithfully represent λ-terms for two reasons.

1. Local variables may appear unbound in sexprs.
    - 'x' is an sexpr, but is not intended to represent any λ-term.
        - Remark: 'X' is an sexpr representing a λ-term with one (particular) global variable.
    - The fix: select the set of sexprs with no unbound local variables.
        - Call this subset *vclosed* for *variable closed*.
    - Substitution is well-behaved on *vclosed*.
2. Different sexprs in *vclosed* may represent the same λ-term.
    - '$[x]x$' and '$[y]y$'; not canonical.
    - The fix: select a canonical subset of *vclosed*.
        - Show that it is an adequate representation of λ-terms.

Overview: Symbolic expressions vs λ-terms

Sexprs do not faithfully represent λ-terms for two reasons.

1. Local variables may appear unbound in sexprs.
    - 'x' is an sexpr, but is not intended to represent any λ-term.
        - Remark: 'X' is an sexpr representing a λ-term with one (particular) global variable.
    - The fix: select the set of sexprs with no unbound local variables.
        - Call this subset *vclosed* for *variable closed*.
    - Substitution is well-behaved on *vclosed* .
2. Different sexprs in *vclosed* may represent the same λ-term.
    - '$[x]x$' and '$[y]y$' ; not canonical.
    - The fix: select a canonical subset of *vclosed* .
        - Show that it is an adequate representation of λ-terms.

Overview: Symbolic expressions vs λ-terms

Sexprs do not faithfully represent λ-terms for two reasons.

1. Local variables may appear unbound in sexprs.
   - 'x' is an sexpr, but is not intended to represent any λ-term.
     - Remark: 'X' is an sexpr representing a λ-term with one (particular) global variable.
   - The fix: select the set of sexprs with no unbound local variables.
     - Call this subset *vclosed* for *variable closed*.
   - Substitution is well-behaved on *vclosed*.

2. Different sexprs in *vclosed* may represent the same λ-term.
   - '$[x]x$' and '$[y]y$'; not canonical.
   - The fix: select a canonical subset of *vclosed*.
     - Show that it is an adequate representation of λ-terms.

Variable-Closed Sexprs

A predicate meaning “no free variables”.

$$\frac{}{\textit{vclosed}\ X} \qquad \frac{\textit{vclosed}\ M \quad \textit{vclosed}\ N}{\textit{vclosed}\ M{\bullet}N} \qquad \frac{\textit{vclosed}\ M}{\textit{vclosed}\ [x][x/X]M}$$

- An abstraction is *vclosed* when . . . .
- Every parameter is *vclosed* and no variable is *vclosed* .
- ‘*vclosed M*’ is provably equivalent to ‘$\mathrm{LV}(M) = \{\}$’.
  - Thus *vclosed* is intuitively correct.
  - Use *vclosed* induction instead of sexpr structural induction . . .
  - . . . no case for unbound variables.

Variable-Closed and Substitution

- Operations $[M/X]N$ and $[M/x]N$ are capture free on *vclosed* .
- *vclosed* is trivially closed under substitution:

$$vclosed\ M \ \wedge\ vclosed\ N \ \Longrightarrow\ vclosed\ [M/X]N$$

- Think of *vclosed* as a “weak typing judgement”.
  - *vclosed* terms behave well for substitution, just as well-typed terms behave well for computation.

Remark: The *vclosed* representation has been used for a big formalisation of type theory [McKinna/Pollack, TLCA’93].

- Remember: *vclosed* representation not canonical.

A Canonical Representation

- Consider again the *vclosed* rules:

$$\frac{}{\textit{vclosed}\ X} \qquad \frac{\textit{vclosed}\ M \quad \textit{vclosed}\ N}{\textit{vclosed}\ M{\cdot}N} \qquad \frac{\textit{vclosed}\ M}{\textit{vclosed}\ [x][x/X]M}$$

  Local variable 'x' not determined in the rule for abstraction.
- To define a canonical subset $\mathbb{L}_\mathrm{F}$, choose 'x' deterministically:

$$\frac{}{X : \mathbb{L}_\mathrm{F}} \qquad \frac{M : \mathbb{L}_\mathrm{F} \quad N : \mathbb{L}_\mathrm{F}}{M{\cdot}N : \mathbb{L}_\mathrm{F}} \qquad \frac{M : \mathbb{L}_\mathrm{F} \quad x = \mathrm{F}_X(M)}{[x][x/X]M : \mathbb{L}_\mathrm{F}}$$

  parameterized by a height function $\mathrm{F} : \mathbb{X} \times \mathbb{S} \to \mathbb{V}$.
- Clearly $M : \mathbb{L}_\mathrm{F} \Longrightarrow \textit{vclosed}\ M$, so substitution is capture free.
- Not obvious that $\mathbb{L}_\mathrm{F}$ is closed under substitution.
- Still to do: specify F such that $\mathbb{L}_\mathrm{F}$ well behaved.

Notation

- Define
$$\mathrm{abs}_X(M) \triangleq [\mathrm{F}_X(M)][\mathrm{F}_X(M)/X]M.$$
Abstraction rule can now be written more abstractly.

$$\frac{}{X : \mathbb{L}_{\mathrm{F}}} \qquad \frac{M : \mathbb{L}_{\mathrm{F}} \quad N : \mathbb{L}_{\mathrm{F}}}{M \cdot N : \mathbb{L}_{\mathrm{F}}} \qquad \frac{M : \mathbb{L}_{\mathrm{F}}}{\mathrm{abs}_X(M) : \mathbb{L}_{\mathrm{F}}}$$

- Everything is now parameterised by a height function F, so drop the explicit subscript.

A Good Height Function

- Interpret $\mathbb{V}$ as $\mathbb{N}$.
- $\mathrm{H} : \mathbb{X} \times \mathbb{S} \to \mathbb{N}$ defined by structural recursion:

$$
\begin{aligned}
\mathrm{H}_X(Y) &\triangleq \begin{cases} 1 & \text{if } X = Y \\ 0 & \text{if } X \neq Y \end{cases} \\
\mathrm{H}_X(x) &\triangleq 0 \\
\mathrm{H}_X(M{\cdot}N) &\triangleq \max(\mathrm{H}_X(M), \mathrm{H}_X(N)) \\
\mathrm{H}_X([x]M) &\triangleq \begin{cases} \mathrm{H}_X(M) & \text{if } \mathrm{H}_X(M) = 0 \text{ or } \mathrm{H}_X(M) > x \\ x + 1 & \text{otherwise} \end{cases}
\end{aligned}
$$

- $\mathbb{L}_\mathrm{H}$ is isomorphic to nominal lambda terms.
- This is too concrete; what properties are really needed?

Three Properties of Good $\mathrm{F} : \mathbb{X} \times \mathbb{S} \to \mathbb{V}$

(HE) F is equivariant:

$$M : \mathbb{L} \implies \mathrm{F}_X(M) = \mathrm{F}_{[\pi]X}([\pi]M).$$

(HP) F is preserved by substitution:

$$M : \mathbb{L} \ \wedge \ Q : \mathbb{L} \ \wedge \ X \neq Y \ \wedge \ X \sharp Q \implies \mathrm{F}_X(M) = \mathrm{F}_X([Q/Y]M).$$

(HF) $\mathrm{F}_X(M)$ does not occur in binding position on any path from the root of M to any occurrence of X in M.

$$M : \mathbb{L} \implies \mathrm{F}_X(M) \notin \mathrm{E}_X(M)$$

where $\mathrm{E}_X(M) : \mathbb{X} \times \mathbb{S} \to (\mathbb{V}\ \mathrm{set})$ is defined:

$$\begin{array}{rcll}
\mathrm{E}_X(\alpha) & \triangleq & \{\} & \text{if } \alpha \text{ is atomic} \\
\mathrm{E}_X(M \bullet N) & \triangleq & \mathrm{E}_X(M) \cup \mathrm{E}_X(N) & \\
\mathrm{E}_X([x]M) & \triangleq & \begin{cases} \{\} & \text{if } X \sharp M \\ \{x\} \cup \mathrm{E}_X(M) & \text{otherwise} \end{cases} &
\end{array}$$

Consistency and Independence of Goodness

- (HE), (HP) and (HF) are consistent: H is good.
- (HE), (HP) and (HF) are independent: no two imply the third.
  - Proof by examples

Now develop a theory of good F sufficient to prove adequacy of the representation.

Many interesting properties follow from goodness of F:

- $\mathbb{L}$ is equivariant: $M : \mathbb{L} \Leftrightarrow [\pi]M : \mathbb{L}$
- Height lemma:

$$\mathrm{F}_X(M) \notin \mathrm{LV}(M) \implies \forall N : \mathbb{L}.\ [N/\mathrm{F}_X(M)][\mathrm{F}_X(M)/X]M = [N/X]M.$$

See most recent paper on my webpage.

Outline

Isomorphism with Nominal Lambda Terms

- Done formally in Isabelle.
  - A, B, C range over nominal terms.
- Define a *representation function* by “primitive recursion”:

$$
\begin{aligned}
!X &\triangleq X \\
!(A \cdot B) &\triangleq !A \cdot !B \\
![X]A &\triangleq \mathrm{abs}_X(!A)
\end{aligned}
$$

  - Need (HE) (F equivariant), to show $!$ is a function.
- Assuming F is good, $!$ is an isomorphic function that preserves substitution:

$$
\begin{array}{rcll}
M : \mathbb{L} & \Longrightarrow & \exists A.\ !A = M & \text{! is surjective,} \\
!A = !B & \Longrightarrow & A = B & \text{! is injective,} \\
!(A[X ::= B]) & = & [!B/X]!A & \text{! respects substitution.}
\end{array}
$$

A Converse: Is Goodness of F Required?

- In this direction we assume $!$ is a substitution preserving isomorphism and have to prove F is good.
- Still working on this.

Outline

Example: β-reduction

$$\frac{[x]P : \mathbb{L} \qquad N : \mathbb{L}}{([x]P)\cdot N \longrightarrow [N/x]P}\ (\beta)$$

$$\frac{M_1 \longrightarrow M_2 \qquad N : \mathbb{L}}{M_1 \cdot N \longrightarrow M_2 \cdot N} \qquad \frac{M : \mathbb{L} \qquad N_1 \longrightarrow N_2}{M \cdot N_1 \longrightarrow M \cdot N_2}$$

$$\frac{M \longrightarrow N}{\mathrm{abs}_x(M) \longrightarrow \mathrm{abs}_x(N)}\ (\xi)$$

- Note rule (ξ) !
  - High level notation $\mathrm{abs}_{\_}(\_)$ hides details.
- $\longrightarrow$ is well behaved, e.g.
  - $\longrightarrow$ is equivariant.
  - $M \longrightarrow N$ implies $M : \mathbb{L}$ and $N : \mathbb{L}$.

Example: Simple Type Assignment

- Let S, T range over *simple types*.
- A *type context*, Γ, is a set of pairs (X, T) such that no two different pairs have the same first component.

$$\frac{(X,T) \in \Gamma}{\Gamma \vdash X : T} \qquad \frac{\Gamma \vdash M : S \to T \quad \Gamma \vdash M : S}{\Gamma \vdash M \cdot N : T}$$

$$\frac{\Gamma \cup (X,S) \vdash M : T}{\Gamma \vdash \mathrm{abs}_X(M) : S \to T}$$

- Type assignment is equivariant.
- $\Gamma \vdash M : T \implies M : \mathbb{L}$.
- To prove weakening of $\vdash$ we must derive a strengthened induction principle, as usual.
  - Nominal Isabelle can do this automatically.

Outline

Conclusion

- Canonical name-carrying representation of binding.
- Well formed terms: inductively defined subset of a datatype.
  - All definitions by structural recursion.
  - All constructors injective.
- More beautiful than [McKinna/Pollack, TLCA'93] …
  - …ours is canonical.
- More beautiful than locally nameless [Ayedemir et al., POPL'08]
  - …name carrying, no indexes.
- Light infrastructure.
  - Formalisable in intensional constructive logic in a few days.
- Large scale use still requires infrastructure.
  - Nominal Isabelle package provides some free automation.