A Canonical [1] Local Representation of Binding

Randy Pollack
LFCS, University of Edinburgh

Masahiko Sato
Graduate School of Informatics, Kyoto University

Version of March 26, 2009

[1] α-equivalence is identity

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

Full paper (submitted):
http://homepages.inf.ed.ac.uk/rpollack/export/SatoPollack09.pdf

Outline

Outline

Local Representations

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

- The idea goes back to Frege, Gentzen and Prawitz.

Different styles:

- Locally named: two species of names.
  - McKinna/Pollack (1993) formalized Pure Type System metatheory.
    - Not canonical representation.
  - This talk: idea of Sato allows canonical representation.
- Locally nameless: names for parameters, de Bruijn indices for locally bound variables.
  - Canonical representation.
  - POPL’08 paper by Ademir, Chargueraud, Pierce, Pollack and Weirich.

Local Representations 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 logics (e.g. Coq).

Some technologies make local representations convenient:

- McKinna/Pollack style strengthened induction and inversion.
- Urban and Pollack, WMM'07, *Strong Induction Principles in the Locally Nameless Representation of Binders*.
- POPL'08 paper by Ademir, Chargueraud, Pierce, Pollack and Weirich.

Outline

Syntax

Names:

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

Symbolic Expressions ($\mathbb{S}[\mathbb{X}]$):

- The syntax of pure λ-terms, ranged over by M, N, P, Q:

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

  - 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 $F_{<:}$,

Occurrences of (Global) Parameters

- Define $X \sharp A$ means *"X does not occur syntactically in A"*.
- We use $X \sharp A$ polymorphically for ...
  - X from any type of parameters
  - A from types of structures: terms, contexts, judgements, ...
- Each instance of $\sharp$ is easily defined by structural recursion.
- In nominal Isabelle, our $\sharp$ corresponds to nominal freshness (also written $\sharp$).
  - Nominal Isabelle provides $\sharp$ polymorphic over classes of atoms and finitely supported structures for free.

Occurrences of Local Variables (LV)

- Defined by structural recursion.
- Respects intended scoping of abstraction.

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

B-Algebras

- A B-algebra is a triple

$$\langle A,\ ()\ : A \times A \to A,\ []\ : \mathbb{N} \times A \to A \rangle$$

  where A is a set containing $\mathbb{N}$ as a subset.
- A B-algebra homomorphism is a function h on B-algebras s.t.:
  1. $h(x) = x \quad$ (h fixes $\mathbb{N}$),
  2. $h((M\ N)) = (h(M)\ h(N))$,
  3. $h([x]M) = [x]h(M)$.

Free B-Algebras: Substitution Abstractly

- $\mathbb{S}[\mathbb{X}]$ is a free B-algebra with free generating set $\mathbb{X}$.

$$\langle \mathbb{S}[\mathbb{X}],\ () : \mathbb{S} \times \mathbb{S} \to \mathbb{S},\ [] : \mathbb{N} \times \mathbb{S} \to \mathbb{S} \rangle$$

- Let B be a B-algebra; any $\rho : \mathbb{X} \to B$ can be uniquely extended to a B-algebra homomorphism $[\rho] : \mathbb{S}[\mathbb{X}] \to B$:
  1. $[\rho]X \triangleq \rho(X)$.
  2. $[\rho]x \triangleq x$.
  3. $[\rho](M\ N) \triangleq ([\rho]M\ [\rho]N)$.
  4. $[\rho][x]M \triangleq [x][\rho]M$.
- In particular, a finite map $\rho : \mathbb{X} \to \mathbb{S}$ is a substitution.
  - $[\rho] : \mathbb{S} \to \mathbb{S}$ is an endomorphism

Substitution, Concretely

- If $\rho : X_i \mapsto M_i$ (and fixes the rest) then $[\rho]$ is concretely defined by *structural* recursion:

$$
\begin{array}{lcl}
[M_i/X_i]x & = & x \\
[M_i/X_i]Y & = & \text{if } X_i = Y \text{ then } M_i \text{ else } Y \\
[M_i/X_i](N_1\ N_2) & = & (([M_i/X_i]N_1)\ [M_i/X_i]N_2) \\
[M_i/X_i]([x]N) & = & [x][M_i/X_i]N
\end{array}
$$

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

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

- Does not prevent capture, e.g. $[x/X][x]X = [x]x$.
  - Will only be use in safe ways.

Equivariance

- $G_{\mathbb{X}}$ group of finite permutations of $\mathbb{X}$ (with composition).
- For $\pi \in G_{\mathbb{X}}$, $[\pi] : \mathbb{S} \to \mathbb{S}$ is a B-algebra automorphism.
- $G_{\mathbb{X}}$ acts on B-algebra $\mathbb{S}[\mathbb{X}]$ by group action $[\pi]M$.
  - $[\pi\sigma]M = [\pi][\sigma]M$,
  - $[\,]M = M$.
- Suppose that $G_{\mathbb{X}}$ acts on two sets U, V.
  - $f : U \to V$ is equivariant if $\forall \pi\, u.\ f([\pi]u) = [\pi]f(u)$.
  - U or V might be a product (e.g. multi-argument f).
  - U or V might have trivial $G_{\mathbb{X}}$ action (e.g. $\mathbb{N}$ or $\mathbb{B}$, truth values).
- If $R : U \to \mathbb{B}$ is an equivariant relation

$$\forall \pi\, u.\ R([\pi]u) = [\pi]R(u) = R(u)$$

  then the relation is preserved by permutations of parameters.
- Can permute parameters in arguments about equivariant relations.

Not Substitution: a purely technical operation

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

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

- Not a B-algebra homomorophism.
  - E.g. doesn’t fix $\mathbb{N}$.
- Does not prevent capture, e.g. $[x/y][x]y = [x]x$.

Outline

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 representing a λ-term with one (particular) global variable.
   - '*x*' is an sexpr, but is not intended to represent any λ-term.
   - The fix: select the set of sexprs with no unbound variables (variable closed, *vclosed*).
   - Substitution is capture-avoiding on *vclosed*.
2. Different sexprs in *vclosed* may represent the same λ-term.
   - '[*x*]*x*' and '[*y*]*y*'
   - The fix: select a canonical subset of *vclosed*.

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 representing a λ-term with one (particular) global variable.
   - 'x' is an sexpr, but is not intended to represent any λ-term.
   - The fix: select the set of sexprs with no unbound variables (variable closed, *vclosed*).
   - Substitution is capture-avoiding on *vclosed*.
2. Different sexprs in *vclosed* may represent the same λ-term.
   - '$[x]x$' and '$[y]y$'
   - The fix: select a canonical subset of *vclosed*.

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 representing a λ-term with one (particular) global variable.
   - 'x' is an sexpr, but is not intended to represent any λ-term.
   - The fix: select the set of sexprs with no unbound variables (variable closed, *vclosed*).
   - Substitution is capture-avoiding on *vclosed*.
2. Different sexprs in *vclosed* may represent the same λ-term.
   - '$[x]x$' and '$[y]y$'
   - The fix: select a canonical subset of *vclosed*.

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 representing a λ-term with one (particular) global variable.
   - 'x' is an sexpr, but is not intended to represent any λ-term.
   - The fix: select the set of sexprs with no unbound variables (variable closed, *vclosed*).
   - Substitution is capture-avoiding on *vclosed*.
2. Different sexprs in *vclosed* may represent the same λ-term.
   - '$[x]x$' and '$[y]y$'
   - The fix: select a canonical subset of *vclosed*.

Variable-Closed Sexprs

A predicate meaning "no free variables".

$$\frac{}{\mathit{vclosed}\ X} \qquad \frac{\mathit{vclosed}\ M \quad \mathit{vclosed}\ N}{\mathit{vclosed}\ (M\ N)} \qquad \frac{\mathit{vclosed}\ M}{\mathit{vclosed}\ [x][x/X]M}$$

- Every parameter is *vclosed* and no variable is *vclosed*.
  - Use *vclosed* induction instead of sexpr structural induction . . .
  - . . . no case for free variables.
- Essential property: *vclosed* is closed under substitution:

  $$\mathit{vclosed}\ M \ \wedge\ \mathit{vclosed}\ N \ \Rightarrow\ \mathit{vclosed}\ [M/X]N$$

  Trivial to prove.

Remark: We could equivalently replace the last rule with

$$\frac{\mathit{vclosed}\ [X/x]M}{\mathit{vclosed}\ [x]M}$$

Variable-Closed Sexprs(2)

- Think of *vclosed* as a “weak typing judgement”.
  - *vclosed* terms behave well for substitution, just as well-typed terms behave well for computation.
- ‘*vclosed M*’ is provably equivalent to ‘$\mathrm{LV}(M) = \{\}$’.
  - Thus *vclosed* is intuitively correct.
  - It is the induction principle for *vclosed* that we want.

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

- The technology of [McKinna/Pollack] is another story . . .
- . . . it is necessary for the present story too.
- Remember: *vclosed* representation not canonical.

A Canonical Representation

- Consider the *vclosed* rules:

$$\frac{}{vclosed\ X} \qquad \frac{vclosed\ M \quad vclosed\ N}{vclosed\ (M\ N)} \qquad \frac{vclosed\ M}{vclosed\ [x][x/X]M}$$

  The variable 'x' is not determined in the rule for abstraction.
- To define a canonical relation $\mathbb{L}$, choose 'x' deterministically:

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

  where $\mathrm{H} : \mathbb{X} \times \mathbb{S} \to \mathbb{N}$ is a function.
- Still to do: define H such that $\mathbb{L}$ is closed under substitution.

The Height Function

$\mathrm{H} : \mathbb{X} \times \mathbb{S} \to \mathbb{N}$ defined by structural recursion:

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

- $\mathrm{H}_X(M) = 0$ iff $X \sharp M$.
- $\mathrm{H}_X(M) = n + 1$ iff X occurs in M, and (writing M as a tree):
  - either $n = 0$ and no path from the root to X goes through a non-zero binder,
  - or n is the largest among all the binders encountered going down the tree from the root to any occurrence of X.

Some Properties of H (on raw sexprs)

- H is equivariant: $\mathrm{H}_X(M) = \mathrm{H}_{[\pi]X}([\pi]M)$.
- $Y \sharp M \;\Rightarrow\; \mathrm{H}_X(M) = \mathrm{H}_Y([Y/X]M)$.
- $X \neq Y \;\wedge\; X \sharp Q \;\Rightarrow\; \mathrm{H}_X([Q/Y]M) = \mathrm{H}_X(M)$.
- A key lemma:

$$x \geq \mathrm{H}_X(M) \;\wedge\; x \notin \mathrm{LV}(M) \;\Rightarrow\; [Z/x][x/X]M = [Z/X]M.$$

  - A common case is when $X = Z$ and we have:

$$x \geq \mathrm{H}_X(M) \;\wedge\; x \notin \mathrm{LV}(M) \;\Rightarrow\; [X/x][x/X]M = M.$$

  - Why the first side condition? $[X/1][1/X]([1]X) = [1]1 \neq [1]X$
  - $x \geq \mathrm{H}_X(M)$ means x does not occur as a binder on any path from the root of M to an occurrence of X .

Equivalent Forms of $\mathbb{L}$

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

- $(*)$ can equivalently be written

$$\frac{X \sharp M \quad [X/x]M : \mathbb{L} \quad x = \mathrm{H}_X([X/x]M)}{[x]M : \mathbb{L}} \quad (**)$$

- In $(**)$ X varies independently of M.
- Any sufficiently fresh X will do in the premises of $(**)$ ...
- ...so the following rule is also equivalent

$$\frac{\forall X.\ (X \sharp M \Rightarrow [X/x]M : \mathbb{L} \wedge x = \mathrm{H}_X([X/x]M))}{[x]M : \mathbb{L}} \quad (***)$$

Some Properties of $\mathbb{L}$

- $\mathbb{L}$ is equivariant: $\quad M : \mathbb{L} \;\Rightarrow\; [\pi]M : \mathbb{L}$
- The following strong induction rule is admissible

$$\frac{\begin{array}{l} (1)\ \forall X.\ \Phi(X) \\ (2)\ \forall M\, N.\ M : \mathbb{L} \wedge \Phi(M) \wedge N : \mathbb{L} \wedge \Phi(N) \Rightarrow \Phi((M\ N)) \\ (3)\ \forall x\, M.\ \ (\forall X.\ X \sharp M \Rightarrow \\ \qquad\qquad x = \mathrm{H}_X([X/x]M) \wedge [X/x]M : \mathbb{L} \wedge \Phi([X/x]M)) \Rightarrow \\ \qquad \Phi([x]M) \end{array}}{\forall N.\ N : \mathbb{L} \Rightarrow \Phi(N)}$$

  - To understand this rule, see [McKinna/Pollack, TLCA'93] or [Ayedemir et.al., POPL'08].
  - Nominal Isabelle can automatically infer a similar strong induction principle.
- Now can prove the key theorem: $\mathbb{L}$ is closed by substitution:

$$M : \mathbb{L} \;\wedge\; N : \mathbb{L} \;\Rightarrow\; [M/X]N : \mathbb{L}$$

Example: β-reduction

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

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

$$\frac{M \longrightarrow N \qquad x = \mathrm{H}_X(M) \qquad y = \mathrm{H}_X(N)}{[x][x/X]M \longrightarrow [y][y/X]N}\ (\xi)$$

- Note change of bound names in rule (ξ) ...
  - ...and side conditions on x and y.
- $\longrightarrow$ 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.

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

$$\frac{\Gamma \cup (X,S) \vdash M : T \qquad x = \mathrm{H}_X(M)}{\Gamma \vdash [x][x/X]M : S \to T}$$

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

Conclusion

- We presented a canonical name-carrying representation of binding.
- Well formed terms are an inductively defined subset of a datatype.
  - All definitions by structural recursion.
- 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.
- Can use nominal Isabelle package for some free automation.