A Canonical [1] Locally Named Representation of Binding

Randy Pollack
LFCS, University of Edinburgh

Masahiko Sato
Graduate School of Informatics, Kyoto University

Version of October 22, 2011

[1] α-equivalence is identity

Details of This Work Available from my Web Page

Available from http://homepages.inf.ed.ac.uk/rpollack/

- These slides
- Isabelle theory files: PollackSatoRicciotti_IsabelleJAR.tgz
- Full paper in JAR: PollackSatoRicciottiJAR.pdf
- Full paper on previous work (in J. Symbolic Computation 45 (2010)): SatoPollack09.pdf

Outline

Outline

Pure Lambda terms: Raw Syntax, naive attempt

- Countable set $\mathbb{X}$ of *atoms* used for *variables*: X, Y, Z.
  - Only relation needed on $\mathbb{X}$ is decidable equality.
- Datatype of *pre-terms* ranged over by M, N, P, Q:

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

- Unfortunately this datatype doesn't respect our idea of binding:
  - $[X]X \neq [Y]Y$ as elements of the datatype.
  - Structural induction doesn't give the right IH.
  - Substitution doesn't behave well on representatives.
- Some approaches:
  - quotient by α-equivalence
  - work with carefully chosen representatives
  - do away with names completely
    - de Bruijn representation
    - Higher Order Abstract Syntax

Distinct species of names

Why is it natural to identify bound names with free names?

- Example: $\rightarrow$-intro rule for simple types

$$(\text{INTRO})\ \frac{\Gamma, X{:}A \vdash b : B}{\Gamma \vdash [X]b : A \rightarrow B}$$

  - 'X' really occurs in the premise.
  - 'X' does not occur in the conclusion.

This suggests:

- Syntactically seperate local (bound) variables from global (free) variables.
- Not a new idea: Frege, Gentzen and Prawitz all informally used different species of names.

Syntax of locally named pre-terms for pure λ

As in McKinna/Pollack [TLCA 1993, JAR 1999].

- 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.

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

- Datatype of pre-terms ranged over by M, N, P, Q:

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

  - No way to bind global names, X.
- 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
  - Corresponds to nominal freshness (also written $\sharp$).

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.

$$[X/X]M = M.$$
$$X \sharp M \implies [P/X]M = M.$$

- 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. $[x/y][x]y = [x]x$.

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, 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*.
2. Different sexprs in 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, 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*.
2. Different sexprs in 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, 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*.
2. Different sexprs in 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”.

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

- *vclosed* terms have no unbound local variables.
- An abstraction is *vclosed* when . . . .
- Every parameter is *vclosed* and no variable is *vclosed* .
- 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* .
  - There are no free local names to get captured!
- *vclosed* is trivially closed under substitution:

$$\textit{vclosed}\ M \ \wedge\ \textit{vclosed}\ N \implies \textit{vclosed}\ [M/X]N$$

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

Applications

- *vclosed* representation used in a big formalisation of type theory [McKinna/Pollack, TLCA'93].
- One other central idea is required for large scale applications:

Topic for Another Talk: Strengthened Induction and Inversion

Many papers:

- McKinna/Pollack [TLCA'93] [JAR 1999].
- Ademir, Chargueraud, Pierce, Pollack and Weirich [POPL'08]
- Berghofer, Norrish and Urban [CADE'07] *Barendregt's Variable Convention in Rule Inductions.*
- Urban and Pollack [WMM'07] *Strong Induction Principles in the Locally Nameless Representation of Binders*.

Limitations of *vclosed* representation

- Feasible way to work with *representatives* of α classes . . .
  - Never needed to define α-conversion in [McKinna/Pollack].
  - Can prove parallel-β-conversion is confluent.
- . . . but Church–Rosser for β-reduction fails on-the-nose for *vclosed* .
  - If we wanted to reason about β-reduction we would need to reason about α-conversion.
- *vclosed* representation not canonical.

A Canonical Locally Named Representation

- Consider again the *vclosed* rules:

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

  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 $M : \mathbb{L}_{\mathrm{F}} \Longrightarrow \mathit{vclosed}\ M$, 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.

Improve Notation

- Everything is parameterised by a height function F; drop explicit subscript.
- Considering rule:

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

define "abstraction":

$$\mathrm{abs}_X M \stackrel{\triangle}{=} [\mathrm{F}_X(M)][\mathrm{F}_X(M)/X]M.$$

- Abstraction rule can now be written more abstractly.

$$\frac{}{X : \mathbb{L}} \qquad \frac{M : \mathbb{L} \qquad N : \mathbb{L}}{M \cdot N : \mathbb{L}} \qquad \frac{M : \mathbb{L}}{\mathrm{abs}_X M : \mathbb{L}}$$

- $\mathrm{abs}_X M$ will behave like informal '$\lambda X.M$'.
  - X does not occur in $\mathrm{abs}_X M$; $\mathrm{abs}_X X \equiv \mathrm{abs}_Y Y$.

A Datatype of Lambda Terms?

Assume good properties for $\mathbb{F}$ (to be discussed below).

- $\mathbb{L}$ can be formalized as a type
  - $\mathbb{L}$ is a decidable predicate on $\mathbb{S}$;
    - can be a proof irrelevant Σ-type in Type Theory.
  - $\mathbb{L}$ is a non-empty predicate on $\mathbb{S}$;
    - can be a defined type in HOL.
- But no amount of clever indexing . . . , inductive-recursive . . . can make $\mathbb{L}$ into a datatype . . .
- . . . because ‘ abs ’ isn’t injective.

Another topic for another talk.

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

(HE) F is equivariant: Let π be a permutation over $\mathbb{X}$, then

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

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

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

Consistency and independence of goodness

- Consistency: A good height function exists.
- Independence: No two of (HE), (HP) and (HF) imply the third.

Proof by examples; see JAR paper.

$\mathrm{abs}_X M$ behaves like abstraction should

We develop a theory of good F. For example:

- From (HE)

$$\text{“}\lambda X.M \overset{\alpha}{\sim} \lambda Y.N'' \implies \mathrm{abs}_X M = \mathrm{abs}_Y N$$

- From (HF)

$$\mathrm{abs}_X M = \mathrm{abs}_Y N \implies \text{“}\lambda X.M \overset{\alpha}{\sim} \lambda Y.N''$$

- From (HP), substitution “under a binder”

$$X \neq Y \ \wedge \ X \sharp Q \implies [Q/Y]\mathrm{abs}_X M = \mathrm{abs}_X [Q/Y]M$$

Together, (HE), (HF) and (HP) show ‘ abs ’ behaves correctly for α -conversion and substitution.

Outline

Is the representation “adequate”?

Formal vs informal Relationship between a formal thing and an informal thing is not formalizable.

Formal vs formal Adequacy of representation of one formal thing by another formal thing depends on which properties we intend to preserve.

We show formally that $\mathbb{L}$ is an adequate representation of pure λ-terms in Nominal Isabelle.

- Let A, B, C range over nominal terms

$$A ::= X \mid B \cdot C \mid [X]A$$

- One more definition: ‘instantiation’ (nominal and Sato terms).

$$([x]M)\triangledown N \stackrel{\triangle}{=} [N/x]M \qquad ([X]A)\blacktriangledown B \stackrel{\triangle}{=} A[X::=B]$$

Isomorphism with Nominal Lambda Terms

- Define a *representation function* by "structural 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 a bijection that preserves substitution and instantiation:

$$\begin{aligned} M : \mathbb{L} &\Longrightarrow \exists A.\ !A = M && !\text{ is surjective,} \\ !A = !B &\Longrightarrow A = B && !\text{ is injective,} \\ !(A[X::=B]) &= [!B/X]!A && !\text{ respects substitution,} \\ !(([X]A)\blacktriangledown Y) &= (\mathrm{abs}_X\,!A)\triangledown Y && !\text{ respects instantiation} \\ & && \quad \text{by parameters.} \end{aligned}$$

A Converse

- Assume $!$ is a bijection that preserves instantiation. Then (HE), (HP) and (HF) hold.
- (Thus preservation of substitution is not independent of the other properties. There is still something to figure out here.)

Outline

Example: β-reduction

$$\frac{P : \mathbb{L} \quad N : \mathbb{L}}{(\mathrm{abs}_X P)\cdot N \to (\mathrm{abs}_X P)\triangledown N}\ (\beta)$$

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

$$\frac{M \to N}{\mathrm{abs}_X M \to \mathrm{abs}_X N}\ (\xi)$$

- $\to$ is well behaved, e.g.
  - $\to$ is equivariant.
  - Reduction and well-formedness: $M \to N \implies M : \mathbb{L} \wedge N : \mathbb{L}$.
  - Reduction respects representation: $A \to B \Leftrightarrow !A \to !B$

Example: Multivariate Lambda Calculus (Pottinger)

Formalized by Wilmer Ricciotti in Matita. Details in JAR paper.

- A single lambda may bind a list of variables.
- $\lambda xy.x \neq \lambda x.\lambda y.x$.
- Redexes have the form $(\lambda x_0 \ldots x_n.M)N_1 \ldots N_n$.
- Contraction is by simultaneous substitution.
- Why? Matches combinator calculus
  - reduction waits for enough arguments.

Multivariate Calculus in Sato style

- Symbolic expressions: values $\mathbb{VS}$; expressions $\mathbb{S}$; lists $\_s$.

$$\frac{}{X : \mathbb{VS}} \qquad \frac{}{(x, n) : \mathbb{VS}} \qquad \frac{M : \mathbb{S}}{[x, n]M : \mathbb{VS}} \qquad \frac{A : \mathbb{VS} \quad Ns : \mathbb{S}s}{A \cdot Ns : \mathbb{S}}$$

- Abstraction carries length of abstracted list.
- Local variable carries index into abstracted list.
- Coerce values to expressions by application to empty list.

BTW, This approach works in locally nameless too.

Well Formed Multivariate terms

- Height function abstracts a list of names atomically: $\mathbb{X}s \times \mathbb{S} \to \mathbb{V}$
- Let $Xs = [X_0, \ldots, X_{n-1}]$, and $f = \mathrm{F}_{Xs}(M) : \mathbb{V}$ for some height function F.
- Let $M = \ldots X_i \ldots X_j \ldots$ contain some of the X_i.
- Abstraction is defined:

$$\mathrm{abs}_{Xs} M \;=\; [f, n] \ldots (f, i) \ldots (f, j) \ldots .$$

- Well formedness:

$$\frac{}{X : \mathbb{VL}_{\mathrm{F}}} \qquad \frac{M : \mathbb{L}_{\mathrm{F}}}{\mathrm{abs}_{Xs} M : \mathbb{VL}_{\mathrm{F}}} \qquad \frac{A : \mathbb{VL}_{\mathrm{F}} \quad \forall N \in Ns.\ N : \mathbb{L}_{\mathrm{F}}}{A \cdot Ns : \mathbb{L}_{\mathrm{F}}}$$

Beta Reduction

- Congruence rules are straightforward, e.g.

$$\frac{A \to A' \qquad N : \mathbb{L}}{A \cdot N \to A' \cdot N} \qquad \frac{M \to N}{\mathsf{abs}_{Xs} M \to \mathsf{abs}_{Xs} N}\ (\xi)$$

- β-rule:
  - applications to too short a vector do not contract, but . . .
  - applications to too long a vector do contract:

$$\frac{\begin{array}{cc} M : \mathbb{L} & Ns = Ns^a @ Ns^b \\ \forall N \in Ns.\ N : \mathbb{L} & \mathsf{lngth}(Xs) = \mathsf{lngth}(Ns^a) \qquad (\mathsf{abs}_{Xs} M) \triangledown Ns^a = A \cdot Qs \end{array}}{(\mathsf{abs}_{Xs} M) \cdot Ns \to A \cdot (Qs @ Ns^b)}\ (\beta)$$

With some messy details, multivariate λ-calculus works.

- Bind a list of names atomically.
- Simultaneous substitution.

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.