

A Canonical ¹ Locally Named Representation of Binding

Randy Pollack

LFCS, University of Edinburgh

Masahiko Sato

Graduate School of Informatics, Kyoto University

Version of November 19, 2009

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: SatoPollackIsabelleJARsubmitted.tgz
- ▶ Full paper submitted: SatoPollackJARsubmitted.pdf
- ▶ Full paper on previous work (to appear in J. Symbolic Computation): SatoPollack09.pdf

Outline

Raw Syntax

Lambda Terms

Variable-Closed Sexprs

Aside: A canonical “locally nameless” representation

A Locally Named Canonical Representation

Adequacy of the Representation

Examples

Conclusion

Outline

Raw Syntax

Lambda Terms

Variable-Closed Sexprs

Aside: A canonical “locally nameless” representation

A Locally Named Canonical Representation

Adequacy of the Representation

Examples

Conclusion

Pure Lambda terms: Raw Syntax, naive attempt

- ▶ Countable set \mathbb{X} of *atoms* used for *variables*: X, Y, Z .
 - ▶ Only relation needed on \mathbb{V} 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 separate 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)
 - ▶ $X \# A$ means “ X does not occur syntactically in A ”.
 - ▶ Easily defined by structural recursion
 - ▶ Corresponds to nominal freshness (also written $\#$).
- ▶ Free occurrences of Local Variables (LV)
 - ▶ Defined by structural recursion.
 - ▶ Respects intended scoping of abstraction.

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

Substitution, Concretely

- ▶ Concretely defined by *structural* recursion:

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

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

$$\begin{aligned}
 [X/X]M &= M. \\
 X \# M &\implies [P/X]M = M.
 \end{aligned}$$

- ▶ **Does not prevent capture**, e.g. $[x/X][x]X = [x]x$.
 - ▶ Will only be use in safe ways.
- ▶ Substitution is a B-algebra homomorphism; 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:

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

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

Outline

Raw Syntax

Lambda Terms

Variable-Closed Sexprs

Aside: A canonical “locally nameless” representation

A Locally Named Canonical Representation

Adequacy of the Representation

Examples

Conclusion

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”.

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

- ▶ An abstraction is *vclosed* when
- ▶ Every parameter is *vclosed* and no variable is *vclosed* .
- ▶ ‘*vclosed M*’ is provably equivalent to ‘ $LV(M) = \{\}$ ’.
 - ▶ 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 $vclosed$.
 - ▶ There are no free local names to get captured!
- ▶ $vclosed$ is trivially closed under substitution:

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

- ▶ 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:

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].
 - ▶ Church–Rosser is on-the-nose for Tait–Martin-Löf parallel reduction.
 - ▶ We could reason about β -conversion (defined in terms of parallel reduction) on-the-nose.
- ▶ ...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.

Aside: “locally nameless”, or locally de Bruijn

- ▶ **Canonical representation**, relatively easy to use.
- ▶ Known to de Bruijn [1972]. Used in implementations: Coq, Lego.
- ▶ Developed formally in Coq: “Engineering Formal Metatheory” [POPL’08].
- ▶ Datatype of *pre-terms* ranged over by M, N, P, Q :

$$M ::= X \mid n \mid P \cdot Q \mid \lambda M$$

- ▶ natural numbers n for local variables
- ▶ Must restrict to “locally closed” pre-terms:
 - ▶ no unbound indices,
 - ▶ $\lambda 0$ is locally closed,
 - ▶ $\lambda 1$ is not locally closed as 1 is not bound locally.
- ▶ No de Bruijn lifting is required!

A Locally Named Canonical Representation

- ▶ Consider again the *vclosed* rules:

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

Local variable 'x' not determined in the rule for abstraction.

- ▶ To define a canonical subset \mathbb{L}_F , **choose 'x' deterministically**:

$$\frac{}{X : \mathbb{L}_F} \quad \frac{M : \mathbb{L}_F \quad N : \mathbb{L}_F}{M \cdot N : \mathbb{L}_F} \quad \frac{M : \mathbb{L}_F \quad x = F_X(M)}{[x][x/X]M : \mathbb{L}_F}$$

parameterized by a **height function** $F : \mathbb{X} \times \mathbb{S} \rightarrow \mathbb{V}$.

- ▶ Clearly $M : \mathbb{L}_F \implies vclosed M$, so substitution is capture free.
- ▶ **Not obvious that \mathbb{L}_F is closed under substitution.**
- ▶ Still to do: **specify F such that \mathbb{L}_F well behaved.**

Improve Notation

- ▶ Everything is parameterised by a height function F ; drop explicit subscript.
- ▶ Define “abstraction”:

$$\text{abs}_X M \triangleq [F_X(M)][F_X(M)/X]M.$$

- ▶ Abstraction rule can now be written more abstractly.

$$\frac{}{X : \mathbb{L}} \quad \frac{M : \mathbb{L} \quad N : \mathbb{L}}{M \cdot N : \mathbb{L}} \quad \frac{M : \mathbb{L}}{\text{abs}_X M : \mathbb{L}}$$

- ▶ $X \# \text{abs}_X M$, just as $X \# \lambda X.M$ in nominal logic or informally.
- ▶ Define “instantiation”:

$$([x]M) \nabla N \triangleq [N/x]M.$$

Instantiation is only applied to abstractions.

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

(HE) F is equivariant:

$$M : \mathbb{L} \implies F_X(M) = F_{\pi \cdot X}(\pi \cdot M).$$

(HP) F is preserved by substitution:

$$M : \mathbb{L} \wedge Q : \mathbb{L} \wedge X \neq Y \wedge X \# Q \implies F_X(M) = F_X([Q/Y]M).$$

(HF) $F_X(M)$ does not occur in binding position on any path from the root of M to any occurrence of X in M .

$$M : \mathbb{L} \implies F_X(M) \notin E_X(M)$$

where $E_X(M) : \mathbb{X} \times \mathbb{S} \rightarrow (\mathbb{V} \text{ set})$ is defined:

$$\begin{aligned} E_X(\alpha) &\triangleq \{\} && \text{if } \alpha \text{ is atomic} \\ E_X(M \cdot N) &\triangleq E_X(M) \cup E_X(N) \\ E_X([x]M) &\triangleq \begin{cases} \{\} & \text{if } X \# M \\ \{x\} \cup E_X(M) & \text{otherwise} \end{cases} \end{aligned}$$

Consistency and independence of goodness

Consistency: A good height function:

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

$$H_X(Y) \triangleq \begin{cases} 1 & \text{if } X = Y \\ 0 & \text{if } X \neq Y \end{cases}$$

$$H_X(x) \triangleq 0$$

$$H_X(M \cdot N) \triangleq \max(H_X(M), H_X(N))$$

$$H_X([x]M) \triangleq \begin{cases} H_X(M) & \text{if } H_X(M) = 0 \text{ or } H_X(M) > x \\ x + 1 & \text{otherwise} \end{cases}$$

Independence: No two of (HE), (HP) and (HF) imply the third.

- ▶ Proof by examples

$\text{abs}_x M$ behaves like abstraction should

- ▶ In nominal logic, or informal notation, λ is not injective

$$\lambda x.x = \lambda y.y$$

- ▶ Defining functions on terms is hard.
- ▶ In our representation \mathbb{S} is a datatype, and the constructor $[_]_$ is injective.

$$[X]M = [Y]N \implies X = Y \wedge M = N$$

- ▶ Defining functions on terms is easy.
- ▶ However, by (HE) (equivariance) have $F_X(X) = F_Y(Y)$. Hence

$$\begin{aligned} \text{abs}_x X &= [F_X(X)][F_X(X)/X]X \\ &= [F_Y(Y)][F_Y(Y)/Y]Y = \text{abs}_y Y. \end{aligned}$$

- ▶ We *construct* the behavior of binding out of ordinary structural and functional operations.

A theory of good height functions

We develop a theory of good F . For example:

- ▶ From (HE)

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

- ▶ From (HF)

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

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

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

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

For details see Pollack/Sato[2009] on my webpage.

A theory of good height functions (2)

- ▶ (HE) shows that ‘abs’ is equivariant:

$$(HE) \wedge M : \mathbb{L} \implies \pi \cdot (\text{abs}_X M) = \text{abs}_{\pi \cdot X} \pi \cdot M.$$

- ▶ (HF) and instantiation:

$$(HF) \wedge (M, N) : \mathbb{L} \implies [N/X]M = (\text{abs}_X M) \nabla N.$$

Outline

Raw Syntax

Lambda Terms

Variable-Closed Sexprs

Aside: A canonical “locally nameless” representation

A Locally Named Canonical Representation

Adequacy of the Representation

Examples

Conclusion

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

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

Isomorphism with Nominal Lambda Terms

- Define a *representation function* by “structural recursion”:

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

- Need (HE) (F equivariant), to show $!$ is a function.
- I’ve hidden some technical details here: see the paper.
- Assuming F is good, $!$ is an isomorphic function that preserves substitution and instantiation:

$$\begin{aligned} M : \mathbb{L} &\implies \exists A. !A = M && ! \text{ is surjective,} \\ !A = !B &\implies A = B && ! \text{ is injective,} \\ !(A[X ::= B]) &= ![B/X]!A && ! \text{ respects substitution,} \\ !(A[X ::= B]) &= (\text{abs}_X !A) \nabla !B. && ! \text{ respects instantiation,} \end{aligned}$$

A Converse

- ▶ Assume $!$ is single valued and preserves substitution and instantiation. Then (HE), (HP) and (HF) hold.
- ▶ The statement of the converse is messy:
 - ▶ Why are instantiation and substitution both required for the converse?
 - ▶ Injectivity of $!$ is *not* required for the converse: it is not independent of the other properties. Why?
- ▶ Still working on this.

Outline

Raw Syntax

Lambda Terms

Variable-Closed Sexprs

Aside: A canonical “locally nameless” representation

A Locally Named Canonical Representation

Adequacy of the Representation

Examples

Conclusion

Example: β -reduction

$$\frac{P : \mathbb{L} \quad N : \mathbb{L}}{(\text{abs}_x P) \cdot N \rightarrow (\text{abs}_x P) \nabla N} \quad (\beta)$$

$$\frac{M_1 \rightarrow M_2 \quad N : \mathbb{L}}{M_1 \cdot N \rightarrow M_2 \cdot N} \quad \frac{M : \mathbb{L} \quad N_1 \rightarrow N_2}{M \cdot N_1 \rightarrow M \cdot N_2} \quad \frac{M \rightarrow N}{\text{abs}_x M \rightarrow \text{abs}_x N} \quad (\xi)$$

- ▶ Expanded form of rule (ξ) :

$$\frac{M \rightarrow N \quad x = F_x(M) \quad y = F_x(N)}{[x][x/X]M \rightarrow [y][y/X]N} \quad (\xi)$$

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

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.

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

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

- ▶ 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

Raw Syntax

Lambda Terms

Variable-Closed Sexprs

Aside: A canonical “locally nameless” representation

A Locally Named Canonical Representation

Adequacy of the Representation

Examples

Conclusion

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.