Strong Normalization for Equi-(Co-)Inductive Types

Andreas Abel

Department of Computer Science
Ludwig-Maximilians-University Munich

TYPES Workshop, 2 May 2007
Cividale, Italy
Introduction

- Theme: Liberate recursive definitions in Type Theory.
- More convenient use of proof assistants.
- Functional programming approach.
- Interesting interplay between recursion/corecursion.
Inductive Types

- Least fixed-points $\mu F$ of monotone type constructors $F$.
- E.g. $\text{List } A = \mu F$ with $F X = 1 + A \times X$.
- Iso-inductive types: Explicit folding and unfolding.

\[
F(\mu F) \xrightarrow{\text{in}} \mu F \xrightarrow{\text{out}} F(\mu F)
\]

\[
\begin{align*}
\text{nil} & := \text{in} \circ \text{inl} : 1 \to \text{List } A \\
\text{cons} & := \text{in} \circ \text{inr} : A \times \text{List } A \to \text{List } A
\end{align*}
\]

- Equi-inductive types: Implicit (deep) folding via type equality.

\[
F(\mu F) = \mu F
\]

\[
\begin{align*}
\text{nil} & := \text{inl} \\
\text{cons} & := \text{inr}
\end{align*}
\]
Motivation

- In normalization proofs, mostly **iso-types** are chosen (Altenkirch [93–99], Barthe et al.[01–06], Geuvers [92], Giménez, Matthes [98], Mendler [87-91]; CIC).
- Notable exceptions: Parigot [92], Raffalli [93–94].
- Iso-types can be trivially simulated by **equi-types**, normalization results can be inherited.
- Equi-types in iso-types only by translation of typing derivations.
- Normalization for equi-types not implied by norm. for iso-types.
- *Loss of structure on terms requires compensating structures on types.*
Inductive Types: Construction From Below

- Least fixed-points can be reached by ordinal iteration:
  \[
  \begin{align*}
  \mu^0 F &= \emptyset \\
  \mu^{\alpha+1} F &= F(\mu^\alpha F) \\
  \mu^\lambda F &= \bigcup_{\alpha < \lambda} \mu^\alpha F
  \end{align*}
  \]

- Size expressions \( a ::= \iota \mid 0 \mid a + 1 \mid \infty \).
- Sized inductive types \( \mu^a F \).
- Laws: \( \beta, \eta \), and
  \[
  \begin{align*}
  \infty + 1 &= \infty \\
  \mu^{a+1} F &= F(\mu^a F).
  \end{align*}
  \]

- \( \text{List}^a A \) contains list of length \( < a \).
Recursion

- General recursion (partial):

\[
\frac{f : A \rightarrow C \vdash t : A \rightarrow C}{\text{fix} \ (\lambda f. t) : A \rightarrow C}
\]

- Recursion on size (total):

\[
\frac{f : \mu^i F \rightarrow C \vdash t : \mu^{i+1} F \rightarrow C}{\text{fix}^\mu (\lambda f. t) : \mu_f F \rightarrow C}
\]
Sized Coinductive Types

- Greatest fixed-points $\nu^\infty F$ of monotone $F$.
- Approximation from above.
- E.g. $\text{Stream}^a A = \nu^a \lambda X. A \times X$ contains streams of depth $\geq a$.
- Corecursion on depth (total):

$$
\frac{f : \nu^i F \vdash t : \nu^{i+1} F}{\text{fix}^\nu (\lambda f.t) : \nu^\infty F}
$$

- E.g., $\text{repeat } x = \text{fix}^\nu (\lambda y. (x, y))$. 

Andreas Abel (LMU Munich)
Terminating Reduction for Recursion

- Naive reduction $\text{fix}^\mu s \rightarrow s (\text{fix}^\mu s)$ diverges.
- Lazy (weak head) values $v ::= (r, s) \mid \cdots \mid \lambda xt \mid \text{fix}^\mu s \mid \text{fix}^\nu s$.
- Only expand recursive functions applied to a value.

\[
\text{fix}^\mu s v \rightarrow s (\text{fix}^\mu s) v
\]

- Shallow evaluation contexts $e(\_):= \text{fst} \_ \mid \cdots \mid \_ s \mid \text{fix}^\mu s \_.$
- Deep evaluation contexts $E(\_)=e_1(\ldots e_n(\_))$ for $n \geq 0$. 

Andreas Abel (LMU Munich)
Termination Reduction for Corecursion

- Only expand corecursive objects whose value is demanded.
  \[ e(fix^\nu s) \rightarrow e(s(fix^\nu s)) \]

- Nonconfluence. Critical pair: \( s = \lambda z \lambda x. x \) and
  \[ fix^\mu s (fix^\nu s) \]

\[
\begin{array}{c}
  s (fix^\mu s) (fix^\nu s) \\
  \downarrow \\
  (\lambda x.x) (fix^\nu s) \\
  \downarrow \\
  fix^\nu s \\
\end{array} \qquad \begin{array}{c}
  fix^\mu s (s(fix^\nu s)) \\
  \downarrow \\
  fix^\mu s (\lambda xx) \\
  \downarrow \\
  fix^\mu s (\lambda xx) \\
  \downarrow \\
  \lambda xx
\end{array}
\]
Breaking the Symmetry

- Do not unfold corecursive arguments of recursive functions.

\[ e(\text{fix}' s) \rightarrow e(s (\text{fix}' s)) \quad e(_) \neq \text{fix}^\mu s' _{\_} \]

- Confluence regained.
- Strong normalization provable.
Proving Strong Normalization

- \( S \) set of strongly normalizing terms.
- Safe (weak head) reduction, preserves s.n. in both directions.

\[
E((\lambda xt) s) \triangleright E([s/x]t) \quad \text{if } s \in SN \\
E(\text{fix}^\mu s v) \triangleright E(s (\text{fix}^\mu s) v) \\
E(e(\text{fix}^\nu s)) \triangleright E(e(s (\text{fix}^\nu s))) \quad \text{if } e(_) \neq \text{fix}^\mu s'
\]

\[
\ldots
\]

reflexivity, transitivity

- \( N = \{ t \mid t \triangleright E(x) \} \) set of neutral terms.
- \( A \) saturated, \( A \in \text{SAT} \), if \( N \subseteq A \subseteq S \) and \( A \) is closed under safe reduction and expansion.

Andreas Abel (LMU Munich)
Soundness of Recursion

Semantical recursion rule:

\[ \forall s \in (\mu^i F \rightarrow C) \rightarrow \mu^{i+1} F \rightarrow C \]

\[ \text{fix}^\mu s \in \mu^\alpha F \rightarrow C \]

Show \( r \in \mu^\alpha F \) implies \( \text{fix}^\mu s \, r \in C \) by induction on ordinal \( \alpha \).

- **Case** \( \alpha = 0 \). Then \( \mu^0 F = N \) and \( r \in N \) implies \( \text{fix}^\mu s \, r \in N \subseteq C \).
- **Case** \( \alpha = \alpha' + 1 \) and \( r \triangleright v \).
  - \( \text{fix}^\mu s \in \mu^{\alpha'} F \rightarrow C \) by induction hypothesis.
  - \( s (\text{fix}^\mu s) \in \mu^{\alpha'+1} F \rightarrow C \) by assumption.
  - \( \text{fix}^\mu s \, r \triangleright s (\text{fix}^\mu s) \, v \in C \).
- **Case** \( \alpha \) limit. By induction hypothesis.
Soundness of Corecursion

Semantical corecursion rule:

\[
\forall \nu. s \in \nu^i F \rightarrow \nu^{i+1} F \\
\frac{}{\text{fix}^\nu s \in \nu^\alpha F}
\]

By induction on \(\alpha\).

- Case \(\alpha = 0\). Then \(\nu^0 F = S\) and \(s \in S\) implies \(\text{fix}^\nu s \in S\).
- Case \(\alpha = \alpha' + 1\).
  - \(\text{fix}^\nu s \in \nu^{\alpha'} F\) by induction hypothesis.
  - \(s (\text{fix}^\nu s) \in \nu^{\alpha' + 1} F\) by assumption.
  - How to prove \(\text{fix}^\nu s \in \nu^{\alpha' + 1} F\)?

Idea: make this additional closure property on saturated sets.
Guarded Saturated Sets

- Consider closure property

\[ s(\text{fix}' s) \in A \text{ implies fix}' s \in A. \]  \hspace{1cm} (1)

- Unsound for \( \mathcal{N} \): must not contain values!
- Otherwise \( \text{fix}\mu s \in \mathcal{N} \rightarrow \mathcal{N} \) fails.
- Solution: define a subclass of guarded saturated sets closed under (1).
Checking Guardedness

- 1, $A \rightarrow B, A \times B, \ldots$ are guarded.
- 0, $\mu^0 F$ are unguarded.
- $\nu^a F$ is guarded if $F 0$ is or $a = 0$.
- $\mu^a F$ is guarded if $F 0$ is and $a = 0$.
- Statically checkable through kinding system with two base kinds $*_u$ (unguarded type) and $*_g$ (guarded type).
- Guardedness is not emptyness: $1 \rightarrow 0$ is empty, but guarded.
Conclusion

- Present work closes gap in my PhD thesis.
- Further work: develop and verify guardedness calculus.
- Test guardedness restriction in practice.
- Acknowledgments:
  
  Guardedness idea arose during invitation to LORIA by Frédéric Blanqui and Colin Riba.