Step-indexed Kripke Models over Recursive Worlds

Lars Birkedal, Bernhard Reus, Jan Schwinghammer, Kristian Støvring, Jacob Thamsborg, Hongseok Yang
Motivation

Modelling realistic programming language features:

- recursive types
- impredicative polymorphism
- dynamic allocation
- higher-order store

\{ \text{ML-style references} \}
Applications

**Unary models**
- type safety
- program logics for higher-order store
- logics for concurrency and storable locks

**Relational models**
- contextual equivalences
  - relational parametricity, data abstraction
- effect-based program transformation
- Benton-style compositional compiler correctness

Modelling involves the construction of recursive structures.
Example: unary model of ML references

**System F with recursive types and ML-style references**

- (cbv) operational semantics

\[
(t \mid h) \mapsto (t' \mid h')
\]

- typing judgements

\[
\Xi; \Gamma \vdash t : \tau
\]

where

\[
\Xi = \alpha_1, \ldots, \alpha_n
\]

\[
\Gamma = \chi_1 : \tau_1, \ldots, \chi_m : \tau_m
\]
Unary model of ML references — ideas

- impredicative polymorphism and recursive types
  - types as predicates over some set of values
- dynamic allocation of references
  - Kripke model where worlds capture information about the heap
  - types as predicates indexed over worlds
- leads to recursive equations

\[
Val = \text{set of values} \\
W = \text{Loc} \to_{\text{fin}} T \\
T = W \to_{\text{mon}} \text{Pred}(Val)
\]

- our approach: solve equations in a category of metric spaces
Contributions

Unification of methods.
- idea first developed using domain-theoretic models
  Birkedal, Støvring & Thamsborg, FOSSACS'09
- we show that it applies to operational semantics
- results in general and abstract account of step-indexing

Applications
- soundness of Charguéraud-Pottier capability type system
- soundness of separation logic with nested triples
Talk outline

1. review: ultrametric spaces
2. step-indexed model of ML references
3. comparison to Indirection Theory
An **ultrametric space** \((X, d)\) satisfies the strong \(\Delta\)-inequality

\[
d(x, z) \leq \max\{d(x, y), d(y, z)\}
\]

A function \(f : X_1 \rightarrow X_2\) is **non-expansive** if

\[
\forall x, y \in X_1 : \ d_2(f(x), f(y)) \leq d_1(x, y)
\]

**CBUlt**: category with

- complete, 1-bounded, non-empty ultrametric spaces and
- non-expansive functions
Function spaces $(X_1, d_1) \to (X_2, d_2)$. 
Non-expansive functions $X_1 \to X_2$ with 

$$d(f, g) = \sup \{d_2(f(x), g(x)) \mid x \in X_1\}$$

Finite functions $Loc \to fin(X, d)$. 
Finite functions $Loc \to fin X$ with 

$$d(f, g) = \begin{cases} 
\max \{d(f(l), g(l)) \mid l\} & \text{if } \text{dom}(f) = \text{dom}(g), \\
1 & \text{otherwise}
\end{cases}$$

Scaling $\delta \cdot (X, d')$. 
Set $X$ with distance function $d(x, x') = \delta \cdot d'(x, x')$
Uniform predicates

Uniform (‘step-indexed’) predicates $p \subseteq \mathbb{N} \times \text{Val}$

**uniformity**

$$(n, v) \in p \land j \leq n \implies (j, v) \in p$$

For such $p, q \in \text{UPred}(\text{Val})$ Appel & McAllester, TOPLAS, 2001 define

**approximation**

$$p[n] = \{ (j, v) \in p \mid j < n \}$$

**distance**

$$d(p, q) = \inf \{ 2^{-n} \mid p[n] = q[n] \}$$

Proposition

*For any set $A$, $\text{UPred}(A) \in \text{CBUlt}$.***
Space of types for ML references

\[ F : \text{CBUlt}^{\text{op}} \times \text{CBUlt} \longrightarrow \text{CBUlt} \]
\[ F(X, Y) = (\text{Loc} \rightarrow_{\text{fin}} X) \rightarrow_{\text{mon}} \text{UPred(Val)} \]

The functor \( \hat{F}(X, Y) = \frac{1}{2} \cdot F(X, Y) \) is locally contractive:

\[ d(\hat{F}(f, g), \hat{F}(f', g')) \leq \frac{1}{2} \cdot \max\{d(f, f'), d(g, g')\} \]

Theorem (America & Rutten 1989)

Every locally contractive functor \( F : \text{CBUlt}^{\text{op}} \times \text{CBUlt} \longrightarrow \text{CBUlt} \) has a unique fixed point \( X \cong F(X, X) \).

In particular, there exists \( \hat{T} \cong \frac{1}{2} \cdot ((\text{Loc} \rightarrow_{\text{fin}} \hat{T}) \rightarrow_{\text{mon}} \text{UPred(Val)}) \).
Interpretation of types

\[ W = \text{Loc} \to_{\text{fin}} \hat{T} \]
\[ T = W \to_{\text{mon}} \text{UPred}(\text{Val}) \]
\[ \text{i.e., } \hat{T} \cong \frac{1}{2} \cdot T \]

Interpretation \([\Xi \vdash \tau] : T^{\Xi} \to T\) by induction:

\[ [\Xi \vdash \alpha]_{\eta}(w) = \eta(\alpha)(w) \]
\[ [\Xi \vdash \tau_1 \times \tau_2]_{\eta}(w) = \{ (n, (v_1, v_2)) | (n, v_i) \in [\Xi \vdash \tau_i]_{\eta}(w) \} \]
\[ \vdots \]
\[ [\Xi \vdash \text{ref } \tau]_{\eta}(w) = \{ (n, l) | l \in \text{dom}(w) \land \forall w' \supseteq w. w(l)(w')[n] = [\Xi \vdash \tau]_{\eta}(w')[n] \} \]
Soundness

Theorem (Type safety)

If $\emptyset \vdash t : \tau$ then $\forall w, n : (n, t) \in \mathcal{E}[\tau](w)$. 

- $\mathcal{E}[\Xi \vdash \tau]_{\eta} : W \rightarrow UPred(Exp)$
  - extends types to expressions
  - ‘step-indexing’ definition, linking $n$ to operational semantics

- $states : W \rightarrow UPred(Heap)$
  - relating worlds with concrete heaps
Well-definedness

Metric space setup as **guiding principle** in step-indexed semantics:

- which steps need be counted to obtain
  - non-expansiveness of $\llbracket \Xi \vdash \tau \rrbracket$
  - non-expansiveness of $\llbracket \Xi \vdash \tau \rrbracket_\eta$
  - non-expansiveness of $E[\llbracket \Xi \vdash \tau \rrbracket_\eta$
  - non-expansiveness of states

- simple calculations
  - essentially the ‘stratification invariant’ of Ahmed, 2004
Specialization to Indirection Theory

**Indirection Theory** Hobor, Dockins & Appel, POPL’10

- general formulation of step-indexed models
- provides *approximate solutions* to recursive equations
- sufficient for many applications

We can derive approximate solutions from metric equations
- detailed statement and formal theorems in our paper

**Corollary**

*Our approach covers step-indexed models described by Indirection Theory.*
Beyond Indirection Theory: recursive operations

Construction of two step-indexed models in our paper

- Charguéraud and Pottier’s capability types ICFP’08, LICS’08
- Separation logic with nested triples Schwinghammer et al., CSL’09

Worlds are world-dependent assertions

\[ W \simeq \frac{1}{2} \cdot W \rightarrow UPred(Heap) \]

together with

- recursive operation \( \circ : W \times W \rightarrow W \) to combine worlds
- defined by Banach fixed point theorem
Ongoing and future work

Systematic treatment of monotonicity
- CBUlt-enriched setting (esp. preordered metric spaces)
  Birkedal, Støvring & Thamsborg, TCS

Application to program logics with Pottier’s anti-frame rules
- ‘carving out’ of worlds as recursive predicates on recursive metric spaces
  Birkedal, Schwinghammer & Støvring, FOSSACS’11

Abstract account of step-indexed models
- models constructed in internal logic of presheaf topos $\mathbf{Set}^{\omega^{op}}$
  Birkedal, Møgelberg, Schwinghammer & Støvring

Formalization in Coq
- CBUlt theory including step-indexed model of ML refs
  Varming et al.