Quantitative classical realizability for imperative side effects and recursive types

Antoine Madet\textsuperscript{1}
joint work with Aloïs Brunel\textsuperscript{2}

\textsuperscript{1}PPS
Université Paris Diderot

\textsuperscript{2}LIPN
Université Paris Nord

DICE 2012
Tallinn, Estonia
Context & Motivation

Elementary Affine Logic
A type system for elementary time normalization.
Context & Motivation

Elementary Affine Logic
A type system for elementary time normalization.

Two ways of proving soundness
Context & Motivation

Elementary Affine Logic
A type system for elementary time normalization.

Two ways of proving soundness

1. **Syntactic** stratification by **depth** level
   + Recursive types
   + Side effects (M. & Amadio 2011)
Context & Motivation

Elementary Affine Logic
A type system for elementary time normalization.

Two ways of proving soundness

1. **Syntactic** stratification by **depth** level
   - Recursive types
   - Side effects (M. & Amadio 2011)

2. Quantitative **realizability** (Dal Lago & Hofmann 2005)
   - Extension to classical realizability (Brunel 2010)
   - Recursive types and side effects
Context & Motivation

Elementary Affine Logic
A type system for elementary time normalization.

Two ways of proving soundness

1. Syntactic stratification by depth level
   + Recursive types
   + Side effects (M. & Amadio 2011)

2. Quantitative realizability (Dal Lago & Hofmann 2005)
   + Extension to classical realizability (Brunel 2010)
   + Recursive types and imperative side effects

Bring stratification into the semantical side!
1 - The elementary type and depth system
The elementary type and depth system

- Take call-by-value $\lambda$-calculus with explicit bang constructors.
The elementary type and depth system

- Take call-by-value λ-calculus with explicit bang constructors.

Types and contexts

\[
A, B ::= \alpha \mid A \to B \mid !A \mid \mu \alpha. A
\]

\[
\Gamma ::= x_1 : (\delta_1, A_1), \ldots, x_n : (\delta_n, A_n)
\]
The elementary type and depth system

- Take call-by-value $\lambda$-calculus with explicit bang constructors.

### Types and contexts

\[
A, B ::= \alpha | A \to B | !A | \mu \alpha. A
\]

\[
\Gamma ::= x_1 : (\delta_1, A_1), \ldots, x_n : (\delta_n, A_n)
\]

### Indexed Judgement

- $\Gamma \vdash^\delta M : A$ where $\delta$ is a depth
- Means $x_i$ occurs at depth $\delta_i$ in $!^\delta M$
The elementary type and depth system

- Take call-by-value $\lambda$-calculus with explicit bang constructors.

Types and contexts

\[ A, B ::= \alpha | A \rightarrow B | !A | \mu\alpha.A \]
\[ \Gamma ::= x_1 : (\delta_1, A_1), \ldots, x_n : (\delta_n, A_n) \]

Indexed Judgement

- $\Gamma \vdash^\delta M : A$ where $\delta$ is a depth
- Means $x_i$ occurs at depth $\delta_i$ in $!^\delta M$

A few rules (based on EAL)

\[
\frac{\Gamma \vdash^{\delta+1} M : A}{\Gamma \vdash^{\delta} !M : !A} \quad \text{prom.}
\]
\[
\frac{\Gamma \vdash^{\delta} M : \mu\alpha.A}{\Gamma \vdash^{\delta} M : A[\mu\alpha.A/\alpha]} \quad \text{unfold.}
\]
The elementary type and depth system

- Take call-by-value $\lambda$-calculus with explicit bang constructors.

Types and contexts

\[
A, B ::= \alpha \mid A \rightarrow B \mid !A \mid \mu\alpha.A
\]

\[
\Gamma ::= x_1 : (\delta_1, A_1), \ldots, x_n : (\delta_n, A_n)
\]

Indexed Judgement

- $\Gamma \vdash^\delta M : A$ where $\delta$ is a depth
- Means $x_i$ occurs at depth $\delta_i$ in $!^\delta M$

Theorem: Elementary bound

- The depth of a typable term does not increase by reduction
- A typable term strongly normalizes in elementary time
2 - Classical realizability
Orthogonality for termination

- $M$ is a term
- $E$ is a call-by-value evaluation context

Define good interaction as

\[ M \perp E \iff E[M] \text{ terminates} \]

Elements of $X \perp \perp$ behave like those of $X$
Orthogonality for termination

- $M$ is a term
- $E$ is a call-by-value evaluation context
- Define good interaction as

$$M \perp E \iff E[M] \text{ terminates}$$

- If $X$ is a set of terms,

$$X^\perp = \{E \mid \forall M \in X, M \perp E\}$$

- Conversely, if $X$ is a set of contexts,

$$X^\perp = \{M \mid \forall E \in X, M \perp E\}$$

Elements of $X^{\perp \perp}$ behave like those of $X$
An indexed interpretation

A naive tentative

- \( \vdash_\delta A \rightarrow B = \{ \lambda x. M \mid \forall V \in \vdash_\delta A, M[V/x] \in \vdash_\delta B \} \perp \perp \)

- \( \vdash_\delta !A = \{ !V \mid V \in \vdash_{\delta + 1} A \} \perp \perp \)

- \( \vdash_\delta \mu \alpha. A = \vdash_\delta A[\mu \alpha. A/\alpha] \)
An indexed interpretation

A naive tentative

- $\vdash_{\delta} A \rightarrow B = \{ \lambda x. M \mid \forall V \in \vdash_{\delta} A, M[V/x] \in \vdash_{\delta} B \} \perp \perp$

- $\vdash_{\delta} ! A = \{ !V \mid V \in \vdash_{\delta+1} A \} \perp \perp$

- $\vdash_{\delta} \mu \alpha. A = \vdash_{\delta} A[\mu \alpha. A/\alpha]$  infinite unfolding!!
An indexed interpretation

A naive tentative

- \( \vdash^\delta A \rightarrow B = \{ \lambda x.M \mid \forall V \in \vdash^\delta A, M[V/x] \in \vdash^\delta B \} \perp \perp \)

- \( \vdash^\delta !A = \{ !V \mid V \in \vdash^{\delta+1} A \} \perp \perp \)

- \( \vdash^\delta \mu\alpha.A = \vdash^\delta A[\mu\alpha.A/\alpha] \)

Idea: stratified recursive types

- Recursive type variables should appear under bangs!
  For example, refuse \( \mu\alpha.A \rightarrow \alpha \) but accept \( \mu\alpha.A \rightarrow !\alpha \).

- Each proof of elementary affine logic has an invariant maximum depth \( d_{\text{max}} \)
An indexed interpretation

A well-defined tentative for some $d_{\text{max}}$

- $\vdash^{\delta} A \rightarrow B = \{ \lambda x.M \mid \forall V \in \vdash^{\delta} A, M[V/x] \in \vdash^{\delta} B \}\perp\perp$

- $\vdash^{\delta} !A = \left\{ \begin{array}{ll} & \{ !V \mid V \in \vdash^{\delta+1} A \}\perp\perp \quad \text{if } \delta < d_{\text{max}} \\ & \text{all terms} \quad \quad \quad \text{if } \delta = d_{\text{max}} \end{array} \right.$

- $\vdash^{\delta} \mu \alpha.A = \vdash^{\delta} A[\mu \alpha.A/\alpha]$ well-founded unfolding

Idea: stratified recursive types

- Recursive type variables should appear under bangs! For example, refuse $\mu \alpha.A \rightarrow \alpha$ but accept $\mu \alpha.A \rightarrow !\alpha$.

- Each proof of elementary affine logic has an invariant maximum depth $d_{\text{max}}$
Towards termination

**Theorem: Adequacy**

If $\neg \vdash^0 M : A$ then $M \in \vdash^0 A$ by taking $d_{max} = d(M)$.

**Corollary: Termination**

- Show $[\cdot] \in \vdash^0 A \perp$
- Hence $M \perp [\cdot]$ which means that $M$ terminates
3 - Towards quantitative classical realizability
Orthogonality for bounded time termination

- $p, q, \ldots$ are natural numbers

- Define bounded time interaction as

  $$(M, p) \perp (E, q) \iff \text{Time}(E[M]) \leq p + q$$
Orthogonality for bounded time termination

- $p, q, \ldots$ are natural numbers

- Define bounded time interaction as
  
  $$(M, p) \perp (E, q) \iff \text{Time}(E[M]) \leq p + q$$

- If $X$ is a set of $(M, p)$,
  
  $$X^\perp = \{ (E, q) \mid \forall (M, p) \in X, (M, p) \perp (E, q) \}$$

- And conversely if $X$ is a set of $(E, q)$

  Elements of $X^{\perp\perp}$ behave like those of $X$
Quantitative interpretation

\[ \vdash^\delta A \rightarrow B = \{(\lambda x. M, p) \mid \forall (V, q) \in \vdash^\delta A, (M[V/x], p + q) \in \vdash^\delta B\}^\perp \]

\[ \vdash^\delta !A = \begin{cases} \{(!V, 2^p) \mid (V, p) \in \vdash^{\delta+1} A\}^\perp & \text{if } \delta < d_{max} \\ \text{all terms} & \text{if } \delta = d_{max} \end{cases} \]
Quantitative interpretation

\[ \vdash^\delta A : B = \{(\lambda x. M, p) \mid \forall (V, q) \in \vdash^\delta A, (M[V/x], p + q) \in \vdash^\delta B\} \perp \perp \]

\[ \vdash^\delta !A = \begin{cases} \{(!V, 2^p) \mid (V, p) \in \vdash^{\delta + 1} A\} \perp \perp & \text{if } \delta < d_{\text{max}} \\ \text{all terms} & \text{if } \delta = d_{\text{max}} \end{cases} \]

**Theorem: Quantitative Adequacy**

If \( \emptyset \vdash^0 M : A \) then there exists some \( p \in \mathbb{N} \) such that \( (M, p) \in \vdash^0 A \) by taking \( d_{\text{max}} = d(M) \).
Quantitative interpretation

$$\vdash_\delta A \rightarrow B = \{(\lambda x. M, p) \mid \forall (V, q) \in \vdash_\delta A, (M[V/x], p + q) \in \vdash_\delta B\} \perp$$

$$\vdash_\delta !A = \begin{cases} 
\{(!V, 2^p) \mid (V, p) \in \vdash_{\delta + 1} A\} \perp & \text{if } \delta < d_{\text{max}} \\
\text{all terms} & \text{if } \delta = d_{\text{max}} 
\end{cases}$$

**Theorem: Quantitative Adequacy**

If $\emptyset \vdash^0 M : A$ then there exists some $p \in \mathbb{N}$ such that $(M, p) \in \vdash^0 A$ by taking $d_{\text{max}} = d(M)$.

**Corollary: Termination in elementary time**

- Because $p$ has the shape of a tower of exponentials of height $d(M) + 1$
- Remark: elements of a so-called **resource monoid** (Dal Lago & Hofmann) should be preferred over natural numbers
4 - A type and depth system with regions
A call-by-value $\lambda$-calculus with regions

Syntax

- A **region** $r$ is a set dynamic values (references, channels, ...)
  
  $r, r', r'', \ldots$
  
  $V ::= \ldots | \star | r$

- A **store** $S$ is a multiset of affectations ($r \leftarrow V$)

Reduction rules

- $E[get(r)], (r \leftarrow V) \rightarrow E[V]$
- $E[set(r, V)] \rightarrow E[\star], (r \leftarrow V)$

- $E$ are weak call-by-value **evaluation contexts**
Types and depth system with regions

Types and contexts

\[ A, B ::= \ldots | 1 | \text{Reg}_r A \]
\[ R ::= r_1 : (\delta_1, A_1), \ldots, r_n : (\delta_n, A_n) \]

Judgement

\[ R; \Gamma \vdash^\delta M : A \]
\[ \text{Means gets/sets on } r_i \text{ occur at depth } \delta_i \text{ in } ![^\delta M \]

A few rules

\[
\frac{r : (\delta, A) \in R}{R; \Gamma \vdash^\delta \text{get}(r) : A}
\]

get

\[
\frac{r : (\delta, A) \in R}{R; \Gamma \vdash^\delta \text{set}(r, V) : 1}
\]

set
Type and depth system with regions

Types and contexts

\[ A, B ::= \ldots | 1 | \text{Reg}_r A \]
\[ R ::= r_1 : (\delta_1, A_1), \ldots, r_n : (\delta_n, A_n) \]

Judgement

\[ R; \Gamma \vdash^\delta M : A \]
\[ \text{Means gets/sets on } r_i \text{ occur at depth } \delta_i \text{ in } !^\delta M \]

Theorem: Elementary bound (M. & Amadio 2011)

\[ \text{The depth of a typable program does not increase by reduction} \]
\[ \text{A typable program normalizes in elementary time} \]
5 - Quantitative classical realizability for regions
Quantitative orthogonality with stores

- A store $S$ should be paired with some weight $s \in \mathbb{N}$
Quantitative orthogonality with stores

- A store $S$ should be paired with some weight $s \in \mathbb{N}$

- Assume $R$ is a set of $(S, s)$, then define $R$-orthogonality as

$$(M, p) \perp_R (E, q) \iff \forall (S, s) \in R, \quad \text{Time}(E[M], S) \leq p + q + s$$

- Define $X \perp_R^R$ using $\perp_R$

Elements of $X \perp_R^R$ behave like those of $X$
Interpretation with stores

What is a set of “good” stores?

Intuitionistic realizability with stores (Boudol’07, Amadio’09)

- Interpret a region context $R$ as a set of stores
- Interpret types with respect to $R$
Interpretation with stores

What is a set of “good” stores?

Intuitionistic realizability with stores (Boudol’07, Amadio’09)

- Interpret a region context $R$ as a set of stores
- Interpret types with respect to $R$

Naive region context interpretation

- $R \vdash^\delta = \left\{ (S, s) \text{ such that } \begin{array}{ll} \bullet & S(r_i) = \{V_i, W_i, \ldots\} \\ \bullet & (V_i, q_i) \in R \vdash^\delta_i A_i \\ \bullet & s = \sum q_i \end{array} \right\}$
- Define type interpretation $R \vdash^\delta A$ using $R \vdash^\delta$-orthogonality
Interpretation with stores

What is a set of “good” stores?

Intuitionistic realizability with stores (Boudol’07, Amadio’09)

- Interpret a region context $R$ as a set of stores
- Interpret types with respect to $R$

Naive region context interpretation

$\vdash^{\delta} R = \left\{ (S, s) \text{ such that} \begin{array}{l} \bullet S(r_i) = \{V_i, W_i, \ldots\} \\ \bullet (V_i, q_i) \in R \vdash^{\delta_i} A_i \\ \bullet s = \sum q_i \end{array} \right\}$

- Define type interpretation $\vdash^{\delta} A$ using $\vdash^{\delta}$-orthogonality

Not well-defined !!
We try to capture circular regions like $(r \leftarrow \lambda x. \text{get}(r) x)$
Stratified regions

Regions types should be guarded by bangs:

\[ R ::= r_1 : (\delta_1, !A_1), \ldots, r_n : (\delta_n, !A_n) \]

A region contains values with side effects on deeper regions only.
Interpretation with stores

Stratified regions

Regions types should be guarded by bangs:

\[ R ::= r_1 : (\delta_1, !A_1), \ldots, r_n : (\delta_n, !A_n) \]

A region contains values with side effects on deeper regions only.

Stratified region context interpretation for \( \delta \leq \delta_i \)

\[ R \vdash^\delta = \left\{ (S, s) \text{ such that }\begin{array}{l}
\bullet S(r_i) = \{!V_i, !W_i, \ldots\} \\
\bullet (V_i, q_i) \in R \vdash^{\delta_i+1} A_i \\
\bullet s = \sum 2^{q_i}
\end{array} \right\} \]

The stored values are adequate to the type of regions since

\( (!V_i, !q_i) \in R \vdash^{\delta_i} !A_i \) by definition
Termination in elementary time with regions

Quantitative adequacy for gets and sets

\[
\begin{align*}
&\triangleright (\text{get}(r), 1) \in R \vdash^\delta !A \\
&\triangleright (\text{set}(r, V), 2 + p_v) \in R \vdash^\delta 1
\end{align*}
\]

Therefore gets/sets consume \textbf{linear} time!

\textbf{Theorem: Elementary bound with regions}

As in the functional case, for a program \( M, S \):

1. Adequacy gives us a \( p \in \mathbb{N} \)

2. \( p \) has the shape of a tower of exponentials of height \( d(M, S) + 1 \)
Conclusion

- An extension of quantitative classical realizability to **recursive types** and **regions** which is sound for Elementary Affine Logic

**Connected approaches to semantic stratification**

- Nakano’s “later” modality ▶ for the stratification of recursive types in an intuitionistic setting
- **Step-indexed** models: approximation of type safety up to $k$ computation steps

**Work in progress…**

- **Polynomial** time: the light resource monoid
- Complexity preserving **monadic translation**
- **Multithreading**
6 - Bonus
Give a region context \( R \), one can define a **state monad**

\[
T_R(A) = \overline{R} \rightarrow \overline{R} \otimes A
\]

where the **store representation** is

\[
\overline{R} = \bigotimes_{r_i \in R} !^i \delta_i X_{r_i}
\]

and each region gives rise to a **recursive equation** on types (Tranquilli 2010):

\[
X_{r_i} = A_i(X_{r_1}, \ldots, X_{r_n})
\]

**Region types** \( A_i \) **should be guarded by bangs!**
The elementary resource monoid (Dal Lago & Hofmann)

- $(M_e, +, 0, \leq)$ is a commutative preordered monoid

- A set $M_e$ of triplets $(l, e, f)$ where
  - $l \in \mathbb{N}$ denotes the linear part of a term
  - $e \in \mathbb{N}$ denotes the exponential part of a term
  - $f$ is a non-decreasing elementary function

- An exponential operation $!: M_e \rightarrow M_e$ defined as
  \[ !(l, e, f) = (1, l + e, x \mapsto f(2^x)) \]

- A function $\| \cdot \| : M_e \rightarrow \mathbb{N}$ to measure triplets:
  \[ \|(a, n, f)\| = f(2^a \cdot n) \]