A General Semantic Construction of Dependent Refinement Type Systems, Categorically

Satoshi Kura

National Institute of Informatics, Tokyo, Japan

The Graduate University for Advanced Studies (SOKENDAI), Kanagawa, Japan

Introduction

Dependent Refinement Type System

Dependent Refinement Type System (DRTS) [Flanagan, POPL'06] is used for verification.

Implementation: LiquidHaskell, F*, ...

DRTSs have

- refinement types,
- dependent types,
- subtyping relation.

Refinement Types

DRTSs have **refinement types** $\{v : A \mid p\}$.

$$\vdash 1 : \{v{:}\mathrm{int} \mid v \geq 0\}$$

$$\nvdash -1 : \{v{:}\mathrm{int} \mid v \geq 0\}$$

$$x : \{v{:}\mathrm{int} \mid v \geq 0\} \vdash 2x : \{w{:}\mathrm{int} \mid w \geq 0\}$$

DRTSs can specify pre-/postconditions.

Dependent Types

DRTSs are **dependently typed**.

$$\vdash \lambda x.x + 1 : (x{:}\mathrm{int}) \to \{v{:}\mathrm{int} \mid v = x + 1\}$$

Postconditions can depend on the input values.

Subtyping Relation

DRTSs have a **subtyping relation** $<:$ induced by logical implication.

$$\frac{v \geq 0 \implies \mathbf{true}}{\vdash \{v{:}\mathbf{int} \mid v \geq 0\} \;<:\; \{v{:}\mathbf{int} \mid \mathbf{true}\}}$$

DRTS Combines Type System and Logic

DRTS

$$x : \{v{:}\mathrm{int} \mid v \geq 0\}$$
$$\vdash x + 1 : \{w : \mathrm{int} \mid w = x + 1\}$$

Underlying Type System (UTS)

$$x : \mathrm{int} \vdash x + 1 : \mathrm{int}$$

DTT (or STT $\hookrightarrow$ DTT)

Predicate Logic

$$v \geq 0$$
$$w = x + 1$$

Our Question

How are UTS, predicate logic, and DRTS related from the viewpoint of categorical semantics?

- As a theoretical framework to handle them in a uniform manner.
- As a guideline to make new DRTSs.
  - With computational effects (= monads)
  - For relational verification

Our Answer: a General Construction

A categorical construction of DRTSs:

$$
\begin{array}{ccc}
 & \text{CCompC} & \\
 & \{\boldsymbol{p} \mid \boldsymbol{q}\} : \{\mathbb{E} \mid \mathbb{P}\} \to \mathbb{P} & \\
 & \text{(model of DRTS)} & \\
\nearrow & & \nwarrow \\
\text{CCompC} & & \text{Posetal fibration} \\
\boldsymbol{p} : \mathbb{E} \to \mathbb{B} & & \boldsymbol{q} : \mathbb{P} \to \mathbb{B} \\
\text{(model of UTS)} & & \text{(model of predicate logic)}
\end{array}
$$

(CCompC: <u>C</u>losed <u>Comp</u>rehension <u>C</u>ategory)

Refined Semantics

$\{p \mid q\}$ gives a (sound) interpretation of DRTS.

$$\text{DRTS} = \text{UTS} + \text{Predicate logic}$$

$$\text{context in } \{p \mid q\} = \text{context in } p + \text{predicate in } q$$

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\}]\!] = ([\![x : \mathrm{int}]\!], [\![x \geq 0]\!])$$

Similarly for types and terms.

$$\text{type in } \{p \mid q\} = \text{type in } p + \text{predicate in } q$$

$$\text{term in } \{p \mid q\} = \text{term in } p + \text{proof in } q$$

Outline

- Interpretation of UTS
  - Example: simple fibration
- Interpretation of predicates
  - Example: subobject fibration
- The construction
  - from simple fibration and subobject fibration

Interpretation of UTS

Interpretation of UTS

UTS = (Martin-Löf) DTT

A (fibrational) model is given by a **closed comprehension category (CCompC)** [Jacobs, TCS'93].

CCompC =
a fibration $p : \mathbb{E} \to \mathbb{B}$ + some conditions

Interpretation in CCompC

Given a CCompC $p : \mathbb{E} \to \mathbb{B}$,

Context: object $[\![\Gamma]\!] \in \mathbb{B}$

Type in context: object $[\![\Gamma \vdash A]\!] \in \mathbb{E}_{[\![\Gamma]\!]}$

Term: morphism in $\mathbb{E}$ or $\mathbb{B}$
(roughly) from $[\![\Gamma]\!]$ to $[\![\Gamma \vdash A]\!]$

Example: Simple Fibration

$s(\mathrm{Set})$ is defined by

- object: (I, X) where $I, X \in \mathrm{Set}$
- morphism: $(u, f) : (I, X) \to (J, Y)$

where $u : I \to J$

and $f : I \times X \to Y$

$$\begin{tikzcd} I \arrow[r, "u"] & J \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

The **simple fibration** $s_{\mathrm{Set}} : s(\mathrm{Set}) \to \mathrm{Set}$ defined by $(I, X) \mapsto I$ is a CCompC.

Example: Interpretation in s_{Set}

Let $\Gamma := x : \mathbf{int}$, $M := x + 1$, $A := \mathbf{int}$.

$[\![\Gamma]\!] = [\![x : \mathbf{int}]\!]$:

$$\mathbb{Z} \in \mathbf{Set}$$

Example: Interpretation in s_{Set}

Let $\Gamma := x : \mathbf{int}$, $M := x + 1$, $A := \mathbf{int}$.

$[\![\Gamma]\!] = [\![x : \mathbf{int}]\!]$:

$$\mathbb{Z} \in \mathbf{Set}$$

$[\![\Gamma \vdash A]\!] = [\![x : \mathbf{int} \vdash \mathbf{int}]\!]$:

$$(\mathbb{Z}, \mathbb{Z}) \in s(\mathbf{Set})$$

Example: Interpretation in s_{Set}

Let $\Gamma := x : \mathbf{int}$, $M := x + 1$, $A := \mathbf{int}$.

$[\![\Gamma]\!] = [\![x : \mathbf{int}]\!]$:

$$\mathbb{Z} \in \mathbf{Set}$$

$[\![\Gamma \vdash A]\!] = [\![x : \mathbf{int} \vdash \mathbf{int}]\!]$:

$$(\mathbb{Z}, \mathbb{Z}) \in s(\mathbf{Set})$$

$[\![\Gamma \vdash M : A]\!] = [\![x : \mathbf{int} \vdash x + 1 : \mathbf{int}]\!]$:

- $(\mathrm{id}_{\mathbb{Z}}, \lambda(x, *).x + 1) \ \in \ s(\mathbf{Set})_{\mathbb{Z}}\big((\mathbb{Z}, 1), (\mathbb{Z}, \mathbb{Z})\big)$
- $\langle \mathrm{id}_{\mathbb{Z}}, \lambda x.x + 1 \rangle : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ in $\mathbf{Set}$

Interpretation of Predicates

Interpretation of Predicates

Model of predicate logic:
a **posetal fibration** (satisfying some conditions).

$$\boldsymbol{q} : \mathbb{P} \to \mathbb{B}$$

Interpretation of a predicate: $[\![\Gamma \vdash \boldsymbol{p}]\!] \in \mathbb{P}_{[\![\Gamma]\!]}$

Example: Interpretation in $\mathrm{sub}_{\mathrm{Set}}$

Given the subobject fibration

$$\mathbf{sub}_{\mathbf{Set}} : \mathbf{Sub}(\mathbf{Set}) \to \mathbf{Set},$$

the predicate $x : \mathbf{int} \vdash x \geq \mathbf{0}$ is interpreted as

$$\begin{aligned} &[\![x : \mathbf{int} \vdash x \geq \mathbf{0}]\!] \\ &= \begin{pmatrix} \{x \in \mathbb{Z} \mid x \geq 0\} \\ \text{\rotatebox{90}{$\subseteq$}} \\ \mathbb{Z} \end{pmatrix} \in \mathbf{Sub}(\mathbf{Set})_{\mathbb{Z}}. \end{aligned}$$

The Construction

CCompC for DRTS

Given

- $s_{\mathrm{Set}} : s(\mathrm{Set}) \to \mathrm{Set}$
- $\mathrm{sub}_{\mathrm{Set}} : \mathrm{Sub}(\mathrm{Set}) \to \mathrm{Set}$,

we construct a CCompC for DRTS
whose total category consists of pairs of

- an underlying type in $s_{\mathrm{Set}} : s(\mathrm{Set}) \to \mathrm{Set}$
- a predicate in $\mathrm{sub}_{\mathrm{Set}} : \mathrm{Sub}(\mathrm{Set}) \to \mathrm{Set}$

Total Category of CCompC for DRTS

We define a category $\{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$ by the pullback.

$$\begin{tikzcd}
\{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\} \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathrm{Sub}(\mathrm{Set})^{\rightarrow} \arrow[d, "\mathrm{sub}^{\rightarrow}_{\mathrm{Set}}"] \\
s(\mathrm{Set}) \arrow[r, "\mathcal{P}"] & \mathrm{Set}^{\rightarrow}
\end{tikzcd}$$

where $\mathcal{P}(I, X) = \pi : I \times X \to I$ is the projection.

Objects in the Total Category

Objects in $\{s(\mathrm{Set}) \mid \mathbf{Sub}(\mathrm{Set})\}$:

$$((I, X), P, Q)$$

where $(I, X) \in s(\mathrm{Set})$ and

$$\begin{tikzcd} Q \arrow[r, dashed] \arrow[d, phantom, "\subseteq" rotate=-90] & P \arrow[d, phantom, "\subseteq" rotate=-90] \\ I \times X \arrow[r, "\pi"] & I \end{tikzcd}.$$

- $(I, X) \in s(\mathrm{Set})$: underlying type
- $P \subseteq I$: predicate on the context
- $Q \subseteq I \times X$: predicate on the type

Definition of CCompC for DRTS

We define

$$\{s_{\mathrm{Set}} \mid \mathrm{sub}_{\mathrm{Set}}\} : \{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\} \to \mathrm{Sub}(\mathrm{Set})$$

by

$$((I, X), P, Q) \mapsto (I, P).$$

Then this gives a CCompC.

Example: Interpretation of Context

In the CCompC $\{s_{\mathrm{Set}} \mid \mathbf{sub}_{\mathrm{Set}}\}$,
a context is interpreted as an object in
the base category $\mathbf{Sub}(\mathbf{Set})$.

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\}]\!] = \begin{pmatrix} \{x \in \mathbb{Z} \mid x \geq 0\} \\ \cap\!\! \mid \\ \mathbb{Z} \end{pmatrix} \in \mathbf{Sub}(\mathbf{Set})$$

Example: Interpretation of Type

A type is interpreted as an object in the total category $\{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$.

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash \{v{:}\mathrm{int} \mid v = x + 1\}]\!]$$

$$\begin{aligned} = ((\mathbb{Z}, \mathbb{Z}), \quad & \{x \in \mathbb{Z} \mid x \geq 0\}, \\ & \{(x, v) \in \mathbb{Z}^2 \mid x \geq 0 \wedge v = x + 1\}) \end{aligned}$$

$$\in \{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$$

Example: Interpretation of Type

A type is interpreted as an object in the total category $\{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$.

$$[\![x : \{x{:}\mathbf{int} \mid x \geq 0\} \vdash \{v{:}\mathbf{int} \mid v = x + 1\}]\!]$$

$$= ((\mathbb{Z}, \mathbb{Z}), \quad \{x \in \mathbb{Z} \mid x \geq 0\}, \\ \{(x, v) \in \mathbb{Z}^2 \mid x \geq 0 \wedge v = x + 1\})$$

$$\in \{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$$

Example: Interpretation of Type

A type is interpreted as an object in the total category $\{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$.

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash \{v{:}\mathrm{int} \mid v = x + 1\}]\!]$$

$$= ((\mathbb{Z}, \mathbb{Z}), \quad \{x \in \mathbb{Z} \mid x \geq 0\}, \quad \{(x, v) \in \mathbb{Z}^2 \mid x \geq 0 \wedge v = x + 1\})$$

$$\in \{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$$

Example: Interpretation of Type

A type is interpreted as an object in the total category $\{s(\mathbf{Set}) \mid \mathbf{Sub}(\mathbf{Set})\}$.

$$\llbracket x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash \{v{:}\mathrm{int} \mid v = x + 1\} \rrbracket$$

$$\begin{aligned} = (&(\mathbb{Z}, \mathbb{Z}), \quad \{x \in \mathbb{Z} \mid x \geq 0\}, \\ &\qquad \{(x, v) \in \mathbb{Z}^2 \mid x \geq 0 \land v = x + 1\}) \end{aligned}$$

$$\in \{s(\mathbf{Set}) \mid \mathbf{Sub}(\mathbf{Set})\}$$

Example: Interpretation of Term

A term is interpreted as a morphism in $\mathbf{Sub}(\mathbf{Set})$ (or $\{s(\mathrm{Set}) \mid \mathbf{Sub}(\mathbf{Set})\}$)

$$\llbracket x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash x+1 : \{v{:}\mathrm{int} \mid v = x+1\} \rrbracket$$

$$= \begin{array}{ccc} \{x \in \mathbb{Z} \mid x \geq 0\} & \dashrightarrow & \{(x,v) \in \mathbb{Z}^2 \mid \begin{array}{l} x \geq 0 \land \\ v = x+1 \end{array}\} \\ \cap\mid & & \cap\mid \\ \mathbb{Z} & \xrightarrow{\langle \mathrm{id},\, \lambda x. x+1 \rangle} & \mathbb{Z}^2 \end{array}$$

Example: Interpretation of Term

A term is interpreted as a morphism in $\mathbf{Sub}(\mathbf{Set})$ (or $\{s(\mathrm{Set}) \mid \mathbf{Sub}(\mathrm{Set})\}$)

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash x + 1 : \{v{:}\mathrm{int} \mid v = x + 1\}]\!]$$

$$= \begin{tikzcd} \{x \in \mathbb{Z} \mid x \geq 0\} \arrow[r, dashed] \arrow[d, phantom, "\cap" rotate=90] & \left\{(x, v) \in \mathbb{Z}^2 \mid \begin{matrix} x \geq 0 \wedge \\ v = x + 1 \end{matrix}\right\} \arrow[d, phantom, "\cap" rotate=90] \\ \mathbb{Z} \arrow[r, "\langle \mathrm{id},\, \lambda x.x+1 \rangle"] & \mathbb{Z}^2 \end{tikzcd}$$

Example: Interpretation of Term

A term is interpreted as a morphism in $\mathbf{Sub}(\mathbf{Set})$ (or $\{s(\mathrm{Set}) \mid \mathbf{Sub}(\mathrm{Set})\}$)

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash x + 1 : \{v{:}\mathrm{int} \mid v = x + 1\}]\!]$$

$$= \begin{tikzcd} \{x \in \mathbb{Z} \mid x \geq 0\} \arrow[r, dashed] \arrow[d, phantom, "\subseteq" rotate=-90] & \left\{(x, v) \in \mathbb{Z}^2 \mid \begin{array}{l} x \geq 0 \wedge \\ v = x + 1 \end{array}\right\} \arrow[d, phantom, "\subseteq" rotate=-90] \\ \mathbb{Z} \arrow[r, "\langle \mathrm{id},\ \lambda x.x+1 \rangle"] & \mathbb{Z}^2 \end{tikzcd}$$

Example: Interpretation of Term

A term is interpreted as a morphism in $\mathrm{Sub}(\mathrm{Set})$ (or $\{s(\mathrm{Set}) \mid \mathrm{Sub}(\mathrm{Set})\}$)

$$[\![\boldsymbol{x} : \{x{:}\mathbf{int} \mid x \geq 0\} \vdash \boldsymbol{x} + \mathbf{1} : \{v{:}\mathbf{int} \mid v = x + 1\}]\!]$$

$$= \begin{array}{ccc} \{x \in \mathbb{Z} \mid x \geq 0\} & \dashrightarrow & \{(x, v) \in \mathbb{Z}^2 \mid \begin{smallmatrix} x \geq 0 \land \\ v = x + 1 \end{smallmatrix}\} \\ \cap\!\!| & & \cap\!\!| \\ \mathbb{Z} & \xrightarrow{\langle \mathbf{id},\ \lambda x. x+1 \rangle} & \mathbb{Z}^2 \end{array}$$

Example: Interpretation of Term

A term is interpreted as a morphism in $\mathbf{Sub}(\mathbf{Set})$ (or $\{s(\mathbf{Set}) \mid \mathbf{Sub}(\mathbf{Set})\}$)

$$[\![x : \{x{:}\mathrm{int} \mid x \geq 0\} \vdash x + 1 : \{v{:}\mathrm{int} \mid v = x + 1\}]\!]$$

$$= \begin{tikzcd} \{x \in \mathbb{Z} \mid x \geq 0\} \arrow[r, dashed] \arrow[d, phantom, sloped, "\subseteq"] & \left\{(x, v) \in \mathbb{Z}^2 \mid \begin{array}{l} x \geq 0 \wedge \\ v = x + 1 \end{array}\right\} \arrow[d, phantom, sloped, "\subseteq"] \\ \mathbb{Z} \arrow[r, "{\langle \mathrm{id},\ \lambda x.x+1 \rangle}"] & \mathbb{Z}^2 \end{tikzcd}$$

Omitted in the Talk

- Generalized construction
  (the intuition is the same).
- Extension of UTS/DRTS with
  - fibred coproduct types $A + B$
  - computational effects (monads)
  - recursion (but this is not completed yet)

Conclusions & Future Work

Conclusions

Given

- $\boldsymbol{p} : \mathbb{E} \to \mathbb{B}$ (CCompC for UTS)
- $\boldsymbol{q} : \mathbb{P} \to \mathbb{B}$ (posetal fibration for predicate logic),

we constructed a CCompC for DRTS

$$\{\boldsymbol{p} \mid \boldsymbol{q}\} : \{\mathbb{E} \mid \mathbb{P}\} \to \mathbb{P}.$$

Future Work

- Complete treatment of recursion
  - Give concrete examples
- Algebraic effects & handlers
- Combining Effect systems

Generalized Construction

Given

- a CCompC $p : \mathbb{E} \to \mathbb{B}$ and
- a posetal fibration $q : \mathbb{P} \to \mathbb{B}$,

we define $\{p \mid q\} : \{\mathbb{E} \mid \mathbb{P}\} \to \mathbb{P}$ by

$$\begin{tikzcd}
\{\mathbb{E} \mid \mathbb{P}\} \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathbb{P}^{\to} \arrow[r, "\mathbf{cod}"] \arrow[d, "q^{\to}"] & \mathbb{P} \\
\mathbb{E} \arrow[r, "\mathcal{P}"] & \mathbb{B}^{\to} &
\end{tikzcd}$$

where $\mathcal{P}X = p\epsilon_X^{\mathbf{1} \dashv \{-\}}$ is the projection.

Main Theorem

If $p : \mathbb{E} \to \mathbb{B}$ is a CCompC and $q : \mathbb{P} \to \mathbb{B}$ is a posetal fibration that is fibred-ccc and has p-products,
then $\{p \mid q\} : \{\mathbb{E} \mid \mathbb{P}\} \to \mathbb{P}$ is a CCompC.

Moreover, there is a morphism of CCompCs from $\{p \mid q\}$ to p.

$$\begin{tikzcd} \{\mathbb{E} \mid \mathbb{P}\} \arrow[r] \arrow[d, "\{p|q\}"'] & \mathbb{E} \arrow[d, "p"] \\ \mathbb{P} \arrow[r] & \mathbb{B} \end{tikzcd}$$