Case Analysis of Higher-Order Data

Joshua Dunfield and Brigitte Pientka

McGill University

LFMTP'08, Pittsburgh, PA, USA

23 June 2008

Higher-Order Abstract Syntax

- Object-level binders as meta-level binders
  - $\forall x.\,(x = 1)$ as $\mathsf{forall}\ \lambda x.(\mathsf{eq}\ x\ 1)$
  - $\mathbf{fn}\ x \Rightarrow x$ as $\mathsf{fn}\ \lambda x.\,x$
- Twelf, λProlog, Elphin, Delphin, Abella, Bedwyr, …

... Beluga

- Data layer (LF) + Computation layer
- A language for programming and writing proofs
- **Explicit** contexts characterized by schemas

Beluga: the usual suspects

- Coverage checking (this paper)
- Termination checking (ongoing work)

Coverage (Closed Data)

Does **case** m **of** Zero $\Rightarrow \ldots$ | Suc $u \Rightarrow \ldots$ cover

$$\text{nat}$$

where

$$\begin{aligned} \text{nat} &: \textbf{type}. \\ \text{Zero} &: \text{nat}. \\ \text{Suc} &: \text{nat} \longrightarrow \text{nat}. \end{aligned} \quad ?$$

- Does every inhabitant of nat match some guard in $\{\text{Zero}, \text{Suc}\ u\}$?

Higher-order Data (Open)

- In contextual modal type theory [Nanevski, Pfenning, Pientka 2008]
- Explicit contexts Ψ:

$$\Psi \quad ::= \quad \cdot \mid \psi \mid \Psi, x{:}A$$

- Context variables ψ range over contexts
- If $m : \mathsf{nat}[\Psi]$ then $\mathbf{FV}(m) \subseteq \mathbf{dom}(\Psi)$

  If $m : \mathsf{nat}[\cdot]$ then $\mathbf{FV}(m) = \emptyset$

  If $m : \mathsf{nat}[\psi, x{:}\mathsf{nat}]$ then $\mathbf{FV}(m) \subseteq \mathbf{dom}(\psi) \cup \{x\}$

Contextual Coverage: Variables

Does

$$\textbf{case } m \textbf{ of box}(x.\,\mathsf{Zero}) \Rightarrow \ldots \mid \textbf{box}(x.\,\mathsf{Suc}\; u[x]) \Rightarrow \ldots$$

cover $\mathsf{nat}[x{:}\mathsf{nat}]$ where

$$\begin{array}{lcl} \mathsf{nat} & : & \textbf{type}. \\ \mathsf{Zero} & : & \mathsf{nat}. \\ \mathsf{Suc} & : & \mathsf{nat} \to \mathsf{nat}. \end{array}$$

?

- Does every inhabitant of nat that is closed with respect to the context x:nat match some guard in $\{x.\,\mathsf{Zero},\; x.\,\mathsf{Suc}\; u[x]\}$?

Contextual Coverage: Variables

Does

$$\textbf{case}\ m\ \textbf{of box}(x.\,\mathsf{Zero}) \Rightarrow \ldots \mid \textbf{box}(x.\,\mathsf{Suc}\ u[x]) \Rightarrow \ldots$$

cover $\mathsf{nat}[x{:}\mathsf{nat}]$ where

$$\begin{array}{lcl} \mathsf{nat} & : & \textbf{type}\,. \\ \mathsf{Zero} & : & \mathsf{nat}\,. \\ \mathsf{Suc} & : & \mathsf{nat} \to \mathsf{nat}\,. \end{array} \quad ?$$

- Does every inhabitant of nat that is closed with respect to the context $x{:}\mathsf{nat}$ match some guard in $\{x.\,\mathsf{Zero},\ x.\,\mathsf{Suc}\ u[x]\}$?
- **No**: misses x

Contextual Coverage: Variables

Does

$$\textbf{case}\ m\ \textbf{of}\ \textbf{box}(x.\,\mathsf{Zero}) \Rightarrow \ldots \mid \textbf{box}(x.\,\mathsf{Suc}\ u[x]) \Rightarrow \ldots$$

$$\mid \textbf{box}(x.\,x) \Rightarrow \ldots$$

cover $\mathsf{nat}[x{:}\mathsf{nat}]$ where

$$\begin{aligned} \mathsf{nat} &: \textbf{type}.\\ \mathsf{Zero} &: \mathsf{nat}.\\ \mathsf{Suc} &: \mathsf{nat} \to \mathsf{nat}. \end{aligned}$$

?

- Does every inhabitant of nat that is closed with respect to the context $x{:}\mathsf{nat}$ match some guard in $\{x.\,\mathsf{Zero},\ x.\,\mathsf{Suc}\ u[x],\ x.\,x\}$?
- Yes (covers x)

Contextual Coverage: Parameters

Does

$$\textbf{case } m \textbf{ of box}(\psi, x.\, \mathsf{Zero}) \Rightarrow \ldots \mid \textbf{box}(\psi, x.\, \mathsf{Suc}\; u[\mathbf{id}_\psi, x]) \Rightarrow \ldots$$
$$\mid \textbf{box}(\psi, x.\, x) \Rightarrow \ldots$$

cover $\mathsf{nat}[\psi, x{:}\mathsf{nat}]$ where

$$\begin{aligned} \mathsf{nat} &: \textbf{type}. \\ \mathsf{Zero} &: \mathsf{nat}. \\ \mathsf{Suc} &: \mathsf{nat} \to \mathsf{nat}. \end{aligned}$$?

- Does every inhabitant of nat that is closed with respect to the context $\psi, x{:}\mathsf{nat}$ match some guard in $\{\psi, x.\, \mathsf{Zero},\quad \psi, x.\, \mathsf{Suc}\; u[x],\quad \psi, x.\, x\}$?

Contextual Coverage: Parameters

Does

$$\textbf{case}\ m\ \textbf{of box}(\psi, x.\ \mathsf{Zero}) \Rightarrow \ldots \mid \textbf{box}(\psi, x.\ \mathsf{Suc}\ u[\textbf{id}_\psi, x]) \Rightarrow \ldots$$
$$\mid \textbf{box}(\psi, x.\ x) \Rightarrow \ldots$$

cover $\mathsf{nat}[\psi, x{:}\mathsf{nat}]$ where

$$\mathsf{nat} : \textbf{type}.$$
$$\mathsf{Zero} : \mathsf{nat}.$$
$$\mathsf{Suc} : \mathsf{nat} \to \mathsf{nat}. \quad ?$$

- Does every inhabitant of nat that is closed with respect to the context $\psi, x{:}\mathsf{nat}$ match some guard in $\{\psi, x.\ \mathsf{Zero},\ \ \psi, x.\ \mathsf{Suc}\ u[x],\ \ \psi, x.\ x\}$?
- **No**: misses variables in ψ

Contextual Coverage: Parameters

Does

$$\textbf{case}\ m\ \textbf{of}\ \textbf{box}(\psi, x.\,\mathsf{Zero}) \Rightarrow \ldots \mid \textbf{box}(\psi, x.\,\mathsf{Suc}\ u[\textbf{id}_\psi, x]) \Rightarrow \ldots$$
$$\mid \textbf{box}(\psi, x.\,x) \Rightarrow \ldots \mid \textbf{box}(\psi, x.\,p[\textbf{id}_\psi]) \Rightarrow \ldots$$

cover $\mathsf{nat}[\psi, x{:}\mathsf{nat}]$ where

$$\begin{array}{lll} \mathsf{nat} & : & \textbf{type}\,. \\ \mathsf{Zero} & : & \mathsf{nat}\,. \\ \mathsf{Suc} & : & \mathsf{nat} \rightarrow \mathsf{nat}\,. \end{array}$$

?

- Does every inhabitant of nat that is closed with respect to the context $\psi, x{:}\mathsf{nat}$ match some guard in $\{\psi, x.\,\mathsf{Zero},\ \ \psi, x.\,\mathsf{Suc}\ u[x],\ \ \psi, x.\,x,\ \ \psi, x.\,p[\textbf{id}_\psi]\}$?
- **Yes**: covers variables in ψ

Outline

- Data and contexts
- Patterns
- Theory of coverage checking
- Summary of results
- Related work

Data

Atomic types	P	$::=$	$a\ M_1 \ldots M_n$
Types	A, B	$::=$	$P \mid \Pi x{:}A.B \mid \Sigma x{:}A.B$
Normal terms	M, N	$::=$	$\lambda x.\, M \mid (M, N) \mid R$
Neutral terms	R	$::=$	$c \mid x \mid u[\sigma] \mid p[\sigma] \mid R\ N \mid \mathbf{proj}_k\, R$
Substitutions	σ	$::=$	$\cdot \mid \sigma\, ;\, M \mid \sigma\, ,\, R \mid \mathbf{id}_\psi$

Data always in canonical form:

$(\lambda x.\, x)c$ ill-formed

Contexts

Atomic types	P	$::=$	$a\ M_1 \ldots M_n$
Types	A, B	$::=$	$P \mid \Pi x{:}A.B \mid \Sigma x{:}A.B$

Contexts	Ψ	$::=$	$\cdot \mid \psi \mid \Psi, x{:}A$
Meta-contexts	Δ	$::=$	$\cdot \mid \Delta, u{::}A[\Psi] \mid \Delta, p{::}A[\Psi]$
Schema contexts	Ω	$::=$	$\cdot \mid \Omega, \psi{::}W$

Context Schemas

Contexts $\Psi \quad ::= \quad \cdot \mid \psi \mid \Psi, x{:}A$

Example context	Schema W
$x{:}\mathsf{nat}, y{:}\mathsf{nat}, z{:}\mathsf{nat}$	$(\mathsf{nat})^*$

Context Schemas

Contexts $\quad \Psi \quad ::= \quad \cdot \mid \psi \mid \Psi, x{:}A$

Example context	Schema W
$x{:}\mathsf{nat}, y{:}\mathsf{nat}, z{:}\mathsf{nat}$	$(\mathsf{nat})^*$
$x{:}\mathsf{bool}, y{:}\mathsf{nat}, z{:}\mathsf{bool}$	$(\mathsf{nat} + \mathsf{bool})^*$

Context Schemas

Contexts $\quad \Psi \quad ::= \cdot \mid \psi \mid \Psi, x{:}A$

Example context	Schema W
$x{:}\mathsf{nat}, y{:}\mathsf{nat}, z{:}\mathsf{nat}$	$(\mathsf{nat})^*$
$x{:}\mathsf{bool}, y{:}\mathsf{nat}, z{:}\mathsf{bool}$	$(\mathsf{nat} + \mathsf{bool})^*$
$xs{:}(\mathsf{list}\ (\mathsf{Suc\ Zero})), ys{:}(\mathsf{list\ Zero})$	$(\mathbf{all}\ n{:}\mathsf{nat}.\mathsf{list}\ n)^*$

Context Schemas

Contexts $\Psi ::= \cdot \mid \psi \mid \Psi, x{:}A$

Example context	Schema W
$x{:}\mathsf{nat}, y{:}\mathsf{nat}, z{:}\mathsf{nat}$	$(\mathsf{nat})^*$
$x{:}\mathsf{bool}, y{:}\mathsf{nat}, z{:}\mathsf{bool}$	$(\mathsf{nat} + \mathsf{bool})^*$
$xs{:}(\mathsf{list}\ (\mathsf{Suc}\ \mathsf{Zero})), ys{:}(\mathsf{list}\ \mathsf{Zero})$	$(\mathbf{all}\ n{:}\mathsf{nat}.\mathsf{list}\ n)^*$
$x{:}\mathsf{nat}, \mathrm{d}{:}(\mathsf{nd}\ (\mathsf{Eq}\ x\ x))$	$(\mathsf{nat} + (\mathbf{all}\ y{:}\mathsf{prop}.\mathsf{nd}\ y))^*$

Context Schemas

Contexts $\Psi ::= \cdot \mid \psi \mid \Psi, x{:}A$

Example context	Schema W
$x{:}\mathsf{nat}, y{:}\mathsf{nat}, z{:}\mathsf{nat}$	$(\mathsf{nat})^*$
$x{:}\mathsf{bool}, y{:}\mathsf{nat}, z{:}\mathsf{bool}$	$(\mathsf{nat} + \mathsf{bool})^*$
$xs{:}(\mathsf{list}\ (\mathsf{Suc\ Zero})), ys{:}(\mathsf{list\ Zero})$	$(\mathbf{all}\ n{:}\mathsf{nat}.\mathsf{list}\ n)^*$
$x{:}\mathsf{nat}, d{:}(\mathsf{nd}\ (\mathsf{Eq}\ x\ x))$	$(\mathsf{nat} + (\mathbf{all}\ y{:}\mathsf{prop}.\mathsf{nd}\ y))^*$
$x{:}(\Sigma n{:}\mathsf{nat}.\mathsf{list}\ n), \ldots$	$(\Sigma n{:}\mathsf{nat}.\mathsf{list}\ n)^*$

Context Schemas

Element types	$\widetilde{A}$	$::=$	$\Pi x{:}A.\widetilde{A} \mid P$
Schema elements	F	$::=$	$\textbf{all}\,\widetilde{\cdots}.\ \Sigma\widetilde{\cdots}.\ \widetilde{A}$
Instance of some F			$\Sigma\widetilde{\cdots}.\ \widetilde{A}$
Schemas	W	$::=$	$(F_1 + \cdots + F_n)^*$

Patterns

Names	$\hat{\Psi}$	$::=$	$\cdot \mid \psi \mid \hat{\Psi}, x$
Patterns	ζ	$::=$	$\Pi\Delta'.\mathbf{box}(\hat{\Psi}.\, M') : A'[\Psi']$
Expressions	e	$::=$	$\mathbf{case}\ e\ \mathbf{of}\ \zeta_1 \Rightarrow e_1 \mid \cdots \mid \zeta_n \Rightarrow e_n$
			$\mid \ \ldots$

Patterns

Names	$\hat{\Psi}$	$::=$	$\cdot \mid \psi \mid \hat{\Psi}, x$
Patterns	ζ	$::=$	$\Pi\Delta'.\mathbf{box}(\hat{\Psi}.\, M') : A'[\Psi']$
Expressions	e	$::=$	$\mathbf{case}\ e\ \mathbf{of}\ \zeta_1 \Rightarrow e_1 \mid \cdots \mid \zeta_n \Rightarrow e_n$
			$\mid \ldots$

$$\zeta \ ::= \ \Pi\, \Delta' \,.\, \mathbf{box}(\hat{\Psi}.\, M') \ : \ A'[\Psi']$$

pattern vars — boxed term — pattern type

Patterns

Names	$\hat{\Psi}$	$::=$	$\cdot \mid \psi \mid \hat{\Psi}, x$
Patterns	ζ	$::=$	$\Pi\Delta'.\mathbf{box}(\hat{\Psi}.\, M') : A'[\Psi']$
Expressions	e	$::=$	$\mathbf{case}\ e\ \mathbf{of}\ \zeta_1 \Rightarrow e_1 \mid \cdots \mid \zeta_n \Rightarrow e_n$
		$\mid$	$\ldots$

$$\zeta ::= \Pi\,\Delta'.\,\mathbf{box}(\hat{\Psi}.\, M') : A'[\Psi']$$

pattern vars — boxed term — pattern type

$$\Pi\, u{::}\mathsf{nat}[\psi, x{:}\mathsf{nat}].\ \mathbf{box}(\psi, x.\ \mathsf{Suc}\ u[\mathbf{id}_\psi, x]) : \mathsf{nat}[\psi, x{:}\mathsf{nat}]$$

Higher-Order Pattern Restriction

$$\zeta ::= \Pi\Delta'.\mathbf{box}(\hat{\Psi}.\, M') : A'[\Psi']$$

- M' is a higher-order pattern (Miller [1991]):
  - pattern variables declared in Δ' applied to distinct sets of bound variables
- hence, pattern variables associated with a renaming substitution

Coverage Judgments

context, continuation

$$\Omega; \Delta; \Psi \vdash \mathsf{Obj}(A) \;\rhd\; \mathcal{J}$$

schema context, meta-context, type

- $\mathsf{Obj}(A) \;\rhd\; \mathcal{J}$: Analyze A, then satisfy $\mathcal{J}$

Coverage Judgments

context — continuation

$$\Omega; \Delta; \Psi \vdash \mathsf{Obj}(A) \;\; \rhd \;\; \mathcal{J}$$

schema context — meta-context — type

- $\mathsf{Obj}(A) \;\; \rhd \;\; \mathcal{J}$: Analyze A, then satisfy $\mathcal{J}$
- $\mathsf{nat}[\psi, x{:}\mathsf{nat}]$ covered by $\{\zeta_1, \ldots, \zeta_n\}$:

$$\psi{:}(\mathsf{nat}{+}\mathsf{bool})^*; \cdot; \psi, x{:}\mathsf{nat} \vdash \mathsf{Obj}(\mathsf{nat}) \rhd \textsc{covered-by}\,\{\zeta_1, \ldots, \zeta_n\}$$

Coverage Judgments

context, continuation

$$\Omega; \Delta; \Psi \vdash \mathsf{Obj}(A) \;\rhd\; \mathcal{J}$$

schema context, meta-context, type

- $\mathsf{Obj}(A) \;\rhd\; \mathcal{J}$: Analyze A, then satisfy $\mathcal{J}$
- $\mathsf{nat}[\psi, x{:}\mathsf{nat}]$ covered by $\{\zeta_1, \ldots, \zeta_n\}$:

$$\psi{:}(\mathsf{nat}{+}\mathsf{bool})^*; \cdot; \psi, x{:}\mathsf{nat} \vdash \mathsf{Obj}(\mathsf{nat}) \rhd \textsc{covered-by}\,\{\zeta_1, \ldots, \zeta_n\}$$

- Rules for $\mathsf{Obj}(\mathsf{nat}) \;\rhd\; \mathcal{J}$ will lead to subderivations $\ldots \vdash M : \mathsf{nat} \;\rhd\; \mathcal{J}$ for various terms M of type nat

Example

- Rules for $\mathsf{Obj}(\mathsf{nat}) \ \triangleright\ \mathcal{J}$ will lead to subderivations $M : A \ \triangleright\ \mathcal{J}$ for various terms M of type nat

$$\Omega = \psi{:}(\mathsf{nat} + \mathsf{bool})^*$$

$$\dfrac{\begin{array}{l}\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{PVars}\langle \psi : \mathsf{nat} \rangle > \mathsf{nat} \ \triangleright\ \mathcal{J} \\ \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{PVars}\langle \psi : \mathsf{bool} \rangle > \mathsf{nat} \ \triangleright\ \mathcal{J} \\ \\ \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle x \rangle (\mathsf{nat} > \mathsf{nat}) \triangleright \mathcal{J} \\ \\ \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{Zero} \rangle\ (\mathsf{nat} > \mathsf{nat}) \triangleright \mathcal{J} \\ \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{Suc} \rangle\ (\mathsf{nat} {\rightarrow} \mathsf{nat} > \mathsf{nat}) \triangleright \mathcal{J} \\ \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{False} \rangle\ (\mathsf{bool} > \mathsf{nat}) \triangleright \mathcal{J} \\ \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{True} \rangle\ (\mathsf{bool} > \mathsf{nat}) \triangleright \mathcal{J}\end{array}}{\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{Obj}(\mathsf{nat}) \ \triangleright\ \mathcal{J}}\ \mathsf{Obj\text{-}split}$$

Example

- Rules for $\mathsf{Obj}(\mathsf{nat}) \;\rhd\; \mathcal{J}$ will lead to subderivations $M : A \;\rhd\; \mathcal{J}$ for various terms M of type nat

$$\Omega = \psi{:}(\mathsf{nat} + \mathsf{bool})^*$$

$$\frac{\begin{array}{l}
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{PVars}\langle \psi : \mathsf{nat} \rangle > \mathsf{nat} \;\rhd\; \mathcal{J} \\
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{PVars}\langle \psi : \mathsf{bool} \rangle > \mathsf{nat} \;\rhd\; \mathcal{J} \\
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle x \rangle (\mathsf{nat} > \mathsf{nat}) \rhd \mathcal{J} \\
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{Zero} \rangle\ (\mathsf{nat} > \mathsf{nat}) \rhd \mathcal{J} \\
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{Suc} \rangle\ (\mathsf{nat} \longrightarrow \mathsf{nat} > \mathsf{nat}) \rhd \mathcal{J} \\
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{False} \rangle\ (\mathsf{bool} > \mathsf{nat}) \rhd \mathcal{J} \\
\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle \mathsf{True} \rangle\ (\mathsf{bool} > \mathsf{nat}) \rhd \mathcal{J}
\end{array}}{\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{Obj}(\mathsf{nat}) \;\rhd\; \mathcal{J}}\ \mathsf{Obj\text{-}split}$$

Example

$$\dfrac{\begin{array}{ll}\Omega \vdash & (\Pi\Delta.\mathbf{box}(\psi, x.\, x) : \mathsf{nat}[\psi, x{:}\mathsf{nat}]) \\ \doteq & (\Pi \cdot .\mathbf{box}(\psi, x.\, x) : \mathsf{nat}[\psi, x{:}\mathsf{nat}])\end{array}}{\vdots} \;\textsf{Covered-By-}\zeta$$

$$\Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{App}\langle x\rangle(\mathsf{nat} > \mathsf{nat}) \rhd \textsc{covered-by}\ \mathsf{Z}$$

- Coverage derivation generates terms that match some pattern $\zeta \in \mathsf{Z}$

Example: Contextual Counting

Checking if x occurs in $e : \mathsf{nat}[\psi, x{:}\mathsf{nat}]$
(sequential matching)

$$
\begin{array}{l}
\textbf{case}\ e\ \textbf{of} \\
\quad \textbf{box}(\psi, x.\, u[\textbf{id}_{\psi}]) \Rightarrow \text{false} \\
\mid \textbf{box}(\psi, x.\, u[x] \quad) \Rightarrow \text{true}
\end{array}
$$

Example: Contextual Counting

Checking if x occurs in $e : \mathsf{nat}[\psi, x{:}\mathsf{nat}]$
(sequential matching)

case e **of**
  $\mathbf{box}(\psi, x.\, u[\mathbf{id}_\psi]) \Rightarrow \text{false}$
| $\mathbf{box}(\psi, x.\, u[x]) \Rightarrow \text{true}$

- Coverage derivation generates terms that **match** some pattern ζ
- Terms must be at least as precise as user's patterns

Example: Contextual Counting

Checking if x occurs in $e : \mathsf{nat}[\psi, x{:}\mathsf{nat}]$ (sequential matching)

$$\begin{array}{l}\textbf{case } e \textbf{ of} \\ \quad \textbf{box}(\psi, x.\, u[\mathbf{id}_\psi]) \Rightarrow \text{false} \\ \mid \textbf{box}(\psi, x.\, u[x] \quad) \Rightarrow \text{true}\end{array}$$

- Coverage derivation generates terms that **match** some pattern ζ
- Terms must be at least as precise as user's patterns
- Coverage rule MVars generates meta-variables $v[\sigma]$ for various σ
  - including $v[\mathbf{id}_\psi]$ and $v[x]$

Summary

- Declarative description of coverage checking for contextual open data
- Algorithm follows from description
  - modulo deciding when to split
- Coverage Soundness:

  If $\ldots \Psi \vdash \mathsf{Obj}(A) \;\triangleright\; \textsc{covered-by}\; Z$ derivable, then every $M : A$ under Ψ is matched by some pattern in Z
- Because we use contextual types with explicit contexts, coverage is **local**

Related Work

Coverage (in related settings)

- Closed data [Coquand 1992,
  Schürmann & Pfenning 2003]
- Open data: regular worlds [Schürmann 2000],
  Delphin worlds [Poswolsky & Schürmann]

Beluga

- [Pientka 2008], [Pientka & Dunfield 2008]

Contextual Modal Type Theory

- [Nanevski, Pfenning, Pientka 2008]

Ongoing Work

- An implementation of coverage checking for Beluga

The End

complogic.cs.mcgill.ca/beluga

Acknowledgments:

- The TPHOLs and LFMTP reviewers

The End

complogic.cs.mcgill.ca/beluga

Acknowledgments:

- The TPHOLs and LFMTP reviewers

The End

complogic.cs.mcgill.ca/beluga

Acknowledgments:

- The TPHOLs and LFMTP reviewers

Example

$$\frac{\Omega;\Delta;\psi,x{:}\mathsf{nat}\vdash \mathsf{nat} \doteqdot \mathsf{nat} \;/\; (\theta,\cdot) \qquad \Omega;\Delta;[\![\theta]\!](\psi,x{:}\mathsf{nat})\vdash [\![\theta]\!]x : [\![\theta]\!]\mathsf{nat} \;\rhd\; [\![\theta]\!]\mathcal{J}}{\Omega;\Delta;\psi,x{:}\mathsf{nat}\vdash \mathsf{App}\langle x\rangle(\mathsf{nat} > \mathsf{nat}) \rhd \mathcal{J}}\;\mathsf{App}\text{-}\doteqdot$$

Example

$$\dfrac{\Omega;\Delta;\psi,x{:}\mathsf{nat} \vdash \mathsf{nat} \doteqdot \mathsf{nat} \;/\; (\cdot,\cdot) \qquad \Omega;\Delta;[\![\cdot]\!](\psi,x{:}\mathsf{nat}) \vdash [\![\cdot]\!]x : [\![\cdot]\!]\mathsf{nat} \;\rhd\; [\![\cdot]\!]\mathcal{J}}{\Omega;\Delta;\psi,x{:}\mathsf{nat} \vdash \mathsf{App}\langle x\rangle(\mathsf{nat} > \mathsf{nat}) \rhd \mathcal{J}}\ \mathsf{App}\text{-}\doteqdot$$

Example

$$\dfrac{\Omega;\Delta;\psi,x{:}\mathsf{nat}\vdash\mathsf{nat}\doteqdot\mathsf{nat}\ /\ (\,\cdot\,,\cdot\,)\qquad \Omega;\Delta;\psi,x{:}\mathsf{nat}\vdash x:\mathsf{nat}\ \rhd\ \mathcal{J}}{\Omega;\Delta;\psi,x{:}\mathsf{nat}\vdash \mathsf{App}\langle x\rangle(\mathsf{nat}>\mathsf{nat})\rhd\mathcal{J}}\ \mathsf{App}\text{-}\doteqdot$$

Example: Contextual Matching

Counting occurrences of x in formulas

$(\mathsf{Eq} : \mathsf{formula} \longrightarrow \mathsf{formula} \longrightarrow \mathsf{formula})$

$\mathbf{case}\ e\ \mathbf{of}$

$\quad \mathbf{box}(\psi, x.\, \mathsf{Eq}\ u[\mathbf{id}_\psi]\quad v[\mathbf{id}_\psi]\quad) \Rightarrow 0$

$\mid \mathbf{box}(\psi, x.\, \mathsf{Eq}\ u[\mathbf{id}_\psi, x]\ v[\mathbf{id}_\psi]\quad) \Rightarrow$ recurse on u

$\mid \mathbf{box}(\psi, x.\, \mathsf{Eq}\ u[\mathbf{id}_\psi]\quad v[\mathbf{id}_\psi, x]) \Rightarrow$ recurse on v

$\mid \mathbf{box}(\psi, x.\, \mathsf{Eq}\ u[\mathbf{id}_\psi, x]\ v[\mathbf{id}_\psi, x]) \Rightarrow$

recurse on u and v, sum results

Example: Contextual Matching

Counting occurrences of x in formulas
($\mathsf{Eq} : \mathsf{formula} \longrightarrow \mathsf{formula} \longrightarrow \mathsf{formula}$)

$$
\begin{array}{l}
\textbf{case } e \textbf{ of} \\
\quad \textbf{box}(\psi, x.\, \mathsf{Eq}\; u[\mathbf{id}_\psi] \quad v[\mathbf{id}_\psi] \quad) \Rightarrow 0 \\
\mid \textbf{box}(\psi, x.\, \mathsf{Eq}\; u[\mathbf{id}_\psi, x]\; v[\mathbf{id}_\psi] \quad) \Rightarrow \text{recurse on } u \\
\mid \textbf{box}(\psi, x.\, \mathsf{Eq}\; u[\mathbf{id}_\psi] \quad v[\mathbf{id}_\psi, x]) \Rightarrow \text{recurse on } v \\
\mid \textbf{box}(\psi, x.\, \mathsf{Eq}\; u[\mathbf{id}_\psi, x]\; v[\mathbf{id}_\psi, x]) \Rightarrow \\
\qquad\qquad \text{recurse on } u \text{ and } v\text{, sum results}
\end{array}
$$

- Coverage derivation generates terms that **match** some pattern ζ
- Terms must be at least as precise as user's patterns

Example: Contextual Matching

$$
\begin{array}{l}
\mathsf{ValidWk}(\mathsf{nat}[\psi, x{:}\mathsf{nat}]) \\
= \\
\begin{array}{llll}
\{\, (\cdot), & \Omega; \Delta, v{::}\mathsf{nat}[\cdot] & ; \Psi \vdash (v[\cdot] & : \mathsf{nat}) \rhd \mathcal{J} \\
\;\; (\psi), & \Omega; \Delta, v{::}\mathsf{nat}[\psi] & ; \Psi \vdash (v[\mathbf{id}_\psi] & : \mathsf{nat}) \rhd \mathcal{J} \\
\;\; (x{:}\mathsf{nat}), & \Omega; \Delta, v{::}\mathsf{nat}[x{:}\mathsf{nat}] & ; \Psi \vdash (v[x] & : \mathsf{nat}) \rhd \mathcal{J} \\
\;\; (\psi, x{:}\mathsf{nat}) \,\} & \Omega; \Delta, v{::}\mathsf{nat}[\psi, x{:}\mathsf{nat}] & ; \Psi \vdash (v[\mathbf{id}_\psi, x] & : \mathsf{nat}) \rhd \mathcal{J}
\end{array} \\
\hline
\qquad\qquad \Omega; \Delta; \psi, x{:}\mathsf{nat} \vdash \mathsf{Obj}(\mathsf{nat}) \;\rhd\; \mathcal{J}
\end{array}
$$