# On the Formalization of Proofs by Logical Relations

Carsten Schürmann and Jeffrey Sarnat
ITU/Yale

September 27, 2006

# Judgmental Reconstruction of Logic

Propositions $A, B ::= o \mid A \supset B$

Judgments Truth : $A$ true

Rules

$$\frac{}{\Gamma, u : A \text{ true}, \Gamma' \vdash u : A \text{ true}}$$

$$\frac{\Gamma, u : A \text{ true} \vdash m : B \text{ true}}{\Gamma \vdash \lambda u : A.\ m : A \supset B \text{ true}} \qquad \frac{\Gamma \vdash m : A \supset B \text{ true} \quad \Gamma \vdash n : A \text{ true}}{\Gamma \vdash m\ n : B \text{ true}}$$

# Judgmental Reconstruction of Uniform Derivations

## Judgments

| | |
|---|---|
| Canonical forms | $\Uparrow A$ |
| Atomic forms | $\downarrow A$ |

## Rules

$$\frac{}{\Gamma, u : \downarrow A, \Gamma' \vdash u : \downarrow A}$$

$$\frac{\Gamma, u : \downarrow A \vdash m : \Uparrow B}{\Gamma \vdash \lambda u : A.\, m : \Uparrow A \supset B} \qquad \frac{\Gamma \vdash m : A \supset \downarrow B \quad \Gamma \vdash n : \Uparrow A}{\Gamma \vdash m\ n : \downarrow B}$$

$$\frac{\Gamma \vdash m : \downarrow o}{\Gamma \vdash m : \Uparrow o}$$

# Definitional Equality

- Weak head reduction: $m \longrightarrow m'$
- Multi-step reduction: $m \longrightarrow^* m'$

$$\frac{}{(\lambda u : A.\, m)\ n \longrightarrow [n/x]m} \qquad \frac{m \longrightarrow m'}{m\ n \longrightarrow m'\ n}$$

$$\frac{}{m \longrightarrow^* m} \qquad \frac{m_1 \longrightarrow^* m_2 \qquad m_2 \longrightarrow^* m_3}{m_1 \longrightarrow^* m_3}$$

# Weak Normalization

**Theorem** If $m : A$ true there exists an $n$, s.t. $m \longrightarrow^* n$ and $n : \Uparrow A$.

**Proof** Define logical relation.

$$
\begin{array}{lll}
\Gamma \vdash m \in [\![o]\!] & \text{iff} & \Gamma \vdash m \longrightarrow^* n \text{ for some } n \\
 & & \text{and } \Gamma \vdash n \Uparrow o \\
\Gamma \vdash m \in [\![A \to B]\!] & \text{iff} & \text{for all } \Gamma' > \Gamma \\
 & & \text{and for all } \Gamma' \vdash n \in [\![A]\!] \\
 & & \text{implies } \Gamma' \vdash m\ n \in [\![B]\!]
\end{array}
$$

Show that if $\Gamma \vdash m : A$ then $\Gamma \vdash m \in [\![A]\!]$.

Show that if $\Gamma \vdash m \in [\![A]\!]$
then $m \longrightarrow^* n$ and $\Gamma \vdash n \Uparrow A$.

$\square$

Logical Framework
Representation of judgments.
Representation of rules.

Assertion Logic
Example: Set Theory

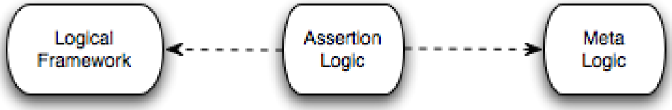
- Set comprehension.
- Trans-finite induction.
- Impredicativity.

Meta Logic
Proof theory of the logical framework.

# Roadmap

- Assertion logic.
- Proof of weak normalization in T welf.
- Proof of weak normalization of System F in Twelf.
- Conclusion.

# Assertion Logic




- Logical framework = Meta logic
  Coq in Coq [Barras, Werner '97]
  Reducibility candidates [Altenkirch '94]
- Logical framework $\neq$ Meta logic
  - Custom design meta logics
    $\mathcal{M}_\omega$, Delphin [CS '01, Poswolsky '06]
    ATS/LF [Xi et al '06]
  - Work with current meta logic
    $\mathcal{M}_2$ [CS '00]
    This work [Sarnat, CS '05]

# Judgmental Reconstruction of Assertion Logic 1

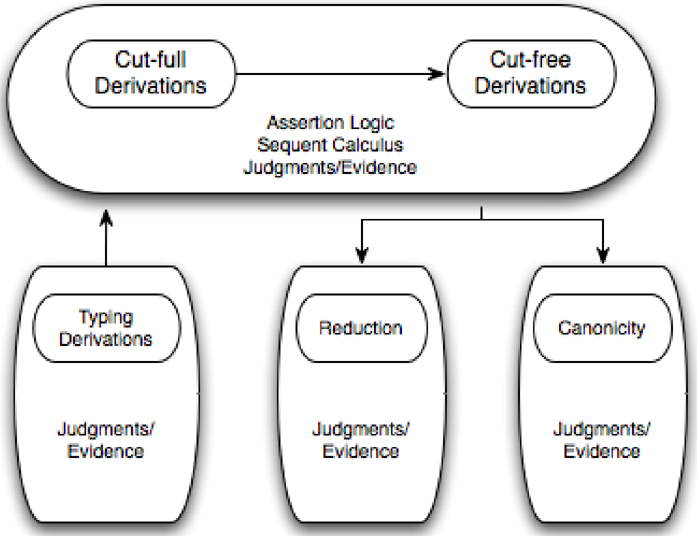
Judgments Sequent calculus [Gentzen '34, Pfenning '95]

```
hyp  : form → type.
conc : form → type.
```

Rules

```
ax : hyp F → conc F.
ir : (hyp F1 → conc F2)
       → conc (F1 ==> F2).
il : conc F1 → (hyp F2 → conc F3)
       → hyp (F1 ==> F2) → conc F3.
fr : (Πm:tm A. conc (F m))
       → conc (forall (λm:tm A. F m)).
fl : ΠM:tm A. (hyp (F1 M) → conc F2)
       → hyp (forall F1) → conc F2.
```

# Overview



Cut-full Derivations
Cut-free Derivations
Assertion Logic
Sequent Calculus
Judgments/Evidence
Typing Derivations
Judgments/ Evidence
Reduction
Judgments/ Evidence
Canonicity
Judgments/ Evidence

# Judgments - as - Propositions

Principle Weak head reduction

$$[\![ m \longrightarrow m' ]\!] = \texttt{wh}\ m\ m'$$

where $\texttt{wh} : \texttt{tm}\ \texttt{A} \rightarrow \texttt{tm}\ \texttt{A} \rightarrow \texttt{form}$

Principle Canonical derivations

$$[\![ \text{exists } n \text{ such that } m \longrightarrow^* n \text{ and } n : \Uparrow A ]\!] = \texttt{hc}\ m$$

where $\texttt{hc} : \texttt{tm}\ \texttt{A} \rightarrow \texttt{form}$

Principle Atomic derivations

$$[\![ \text{exists } n \text{ such that } m \longrightarrow^* n \text{ and } n : \downarrow A ]\!] = \texttt{ha}\ m$$

where $\texttt{ha} : \texttt{tm}\ \texttt{A} \rightarrow \texttt{form}$

# Judgmental Reconstruction of Assertion Logic 2

Right Rules

```
s1 : conc (wh (app (lam M) N) (M N)).
s2 : conc (wh M M')
        → conc (wh (app M N) (app M' N)).
s3: (Πx:tm A. hyp (ha x)
          → conc (hc (app M x)))
        → conc (hc M).
s4: ΠM:tm o.conc (wh M M') → conc (hc M')
        → conc (hc M).
s5: ΠM:tm o. conc (ha M)
        → conc (hc M).
s6: conc (hc N) → conc (ha M)
        → conc (ha (app M N)).
```

# Logical Relation

**Definition**
$$\Gamma \vdash m \in [\![o]\!] \quad \text{iff} \quad \Gamma \vdash m \longrightarrow^* n \text{ for some } n \text{ and } \Gamma \vdash n \Uparrow o$$
$$\Gamma \vdash m \in [\![A \to B]\!] \quad \text{iff} \quad \text{for all } \Gamma' > \Gamma \text{ and for all } \Gamma' \vdash n \in [\![A]\!] \text{ implies } \Gamma' \vdash m\ n \in [\![B]\!]$$

**Encoding** `lr : ΠA:tp. (tm A → form) → type.`

```
lr_o : lr o (λm:tm o. hc m).
lr_arr : lr A LR1 → lr B LR2
         → lr (A => B)
            (λm:tm (A => B).
              forall (λn:tm A.
              LR1 n ==> LR2 (app m n))).
```

# Fundamental Theorem

**Theorem** If $\Gamma \vdash m : A$ then $\Gamma \vdash m \in [\![A]\!]$.

**Proof** by induction on m.

**Comment** Sequent calculus + cut: `conc* : form` $\rightarrow$ type.

```
fund : ΠM:tm A. lr A LR → conc* (LR M) → type.
```

# Closure under Weak-Head Expansion

Theorem If $\Gamma \vdash m \in [\![A]\!]$ and $m' \longrightarrow m$ then $\Gamma \vdash m' \in [\![A]\!]$.

Proof by induction $A$.

```
cwhe : lr A LR
       → conc* (forall (λm:tm A. forall (λm':tm A.
                wh m' m ==> LR m ==> LR m'))) → type.
```

# Escape Theorem

**Theorem**

1. If $\Gamma \vdash m \in [\![A]\!]$ then $\Gamma \vdash m \Uparrow N$ for some canonical $N$.
2. If $\Gamma \vdash m \downarrow$ then $\Gamma \vdash m \in [\![A]\!]$.

```
escape1 : lr A LR
       → conc* (forall (λm:tm A. LR m ==> hc m))
       → type.

escape2 : lr A LR
       → conc* (forall (λm:tm A. ha m ==> LR m))
       → type.
```

# Propositions - as - Judgments

**Theorem**

1. If conc (hc m) then $m \longrightarrow^* n$ and $n : \Uparrow A$.
2. If conc (ha m) then $m \longrightarrow^* n$ and $n : \downarrow A$.
3. If conc (wh m m') then $m \longrightarrow m'$.

**Discussion**

1. Works because the assertion logic is sound.
2. Cut-elimination implies soundness.
3. Syntactic soundness proof. [Pfenning '95]

**Theorem** Cut elimination

```
ce : conc* F → conc F → type.
```

□

# Role of the Meta-Logic

**Conjecture** Predicates - as - judgments sound and complete only if the assertion logic is consistent.

**Observations** Judgments - as - propositions enhances assertion logic by new axioms.

- Right rules: new right commutative conversions. [Sarnat, CS '05]
- Left and right rules: much more complicated. [Miller, McDowell '00]

**Worry** Gödels second incompleteness theorem.

# Pushing the Envelope: System F

**Extension** Assertion logic + second order quantifiers.

$$\texttt{forall}_2\texttt{r} : (\Pi \texttt{p}{:}\texttt{tm A} \rightarrow \texttt{form. conc (F p))} \\ \rightarrow \texttt{conc (forall}_2\ \texttt{F)}.$$

$$\texttt{forall}_2\texttt{l} : \Pi \texttt{P}{:}\texttt{tm A} \rightarrow \texttt{form. (hyp (F P)} \rightarrow \texttt{conc F}_2\texttt{)} \\ \rightarrow \texttt{hyp (forall}_2\ \texttt{F)} \rightarrow \texttt{conc F}_2.$$

**Good news** In Twelf: Weak normalization of System F.

**Bad news** No syntactic consistency proof of assertion logic known.

[Tait 66, Takahashi 67, Girard 88]

**Good news** Cut-elimination procedure can be implemented.

## Twelf's Meta Logic

**Semantics** For all LF types $\Gamma \vdash A$ : type is there an LF object $M$ and a LF substitution $\cdot \vdash \sigma : \Gamma$, s.t. $\cdot \vdash M : A[\sigma]$.

**Justification** Soundness by realizability interpretation.

$$\text{Totality} = \text{Coverage} + \text{Termination}$$

**But...**

$$S(\mathcal{M}_2) < \epsilon_0 < \Psi(\epsilon_{\Omega+1}) < S(\mathcal{SOL})$$

[Fefermann, Pohlers, Schütte et al.]

# Conclusion

| | |
|---|---|
| Summary | Twelf supports proofs by logical relations. |
| | Judgments - as - propositions. |
| | Propositions - as - judgments. |
| | Consistency of the assertion logic. |
| | Termination up to $\epsilon_0$. |
| | Executable cut-elimination proof. |
| | Explicit meta-theoretic assumptions. |
| | Modular assertion logic design. |
| Future work | Twelf's proof - theoretic strength. |