Logical- and Meta-Logical Frameworks Lecture 1

Carsten Schürmann

August 3, 2006

Carsten Schürmann Logical- and Meta-Logical Frameworks Lecture 1

▲ 臣 ▶ | ▲ 臣 ▶

Welcome

(ロ) (四) (E) (E) (E)

- 1. From philosophical considerations to inductive proofs.
- 2. The Edinburgh logical framework.
- 3. The Twelf meta-logical framework.
- 4. An extended example: formalization of cut elimination.
- 5. Inductive proofs and beyond.

向下 イヨト イヨト

- Solid understanding of the underlying ideas.
- Use Twelf.
- Compare Twelf to Coq, Lego, Isabelle/HOL, Nurpl.
- Compare it Maude, Elan.
- Participate in POPLmark challenge.

向下 イヨト イヨト

First possibility: Proposition of some logic \mathcal{L} .

- Examples: even(x), prime(x).
- ▶ Requires: We accept *L* as sound.
- ▶ But: *L* classical, intuitionistic, linear, relevant, modal?
- Philosophical problem: Proposition $true(\mathcal{L}, A)$.

向下 イヨト イヨト

Second possibility: Judgments

[Martin-Löf]

(4) (5) (4) (5) (4)

- Constructivism
- Judgments: Facts that we want to establish as true
- Evidence: Witness the fact of judgments being true

Examples of judgments:

A wff E evaluates to V E is a well-typed expression of type T Definition: Schematic variables: A, V, T More concise: Family of judgments.

向下 イヨト イヨト

Running example: Propositional logic.

 $A, B ::= P \mid A \land B \mid A \lor B \mid \neg B \mid A \supset B$

defines implicitly the judgment wff. Judgment: *A* true

Intuitionistic Logic $A \lor \neg A$ true is not valid. Classical Logic $A \lor \neg A$ true is valid.

・吊り ・ヨト ・ヨト ・ヨ

$\begin{array}{c} \mathcal{D} \\ \text{Notation We write } \mathcal{J} \text{ or } \mathcal{D} :: \mathcal{J} \text{ for the evidence that } \mathcal{J} \text{ is valid.} \\ \\ \hline \\ \text{Construction} \\ \hline \\ \frac{\mathcal{D}_1 \qquad \mathcal{D}_n}{\mathcal{J}_1 \qquad \cdots \qquad \mathcal{J}_n} \\ \text{Summary Constructive way to obtain evidence. Reasoning principles come for free.} \\ \end{array}$

4 B M 4 B M

Judgment: A true.



Remark: Rules have schematic variables.

高 とう ヨン うまと

æ

$\frac{1}{A \text{ true}} u$ \mathcal{D} B true

u is the name of the hypothesis.

 $\ensuremath{\mathcal{D}}$ is hypothetic evidence assuming evidence for A true.

Hypothetical judgment's validity may rely on hypothetical evidence.

向下 イヨト イヨト

Hypothetical judgment (cont'd)



- - E + - E +



Natural deduction semantics[Gentzen '34]Other connectives can be declared and defined.

同 と く ヨ と く ヨ と …

Comments on notation.

Many roads lead to Rome. Contexts range over sets of assumptions.

$$\frac{\Gamma, p :: \text{wff}, u :: A \text{ true} \vdash p \text{ true}}{\Gamma \vdash \neg A \text{ true}} \operatorname{negl}^{p, u} = \frac{\Gamma, A \vdash p}{\Gamma \vdash \neg A} \operatorname{negl}^{p, u}$$

Today you can think this way.

Tomorrow you have to think the hypothetical way.

向下 イヨト イヨト

Can you find some evidence \mathcal{D} that

 $\frac{1}{A \text{ true}} u$ \mathcal{D} $\neg \neg A \text{ true}$

(本部) (本語) (本語) (語)

Lemma: There exists evidence \mathcal{D} , such that

 $\frac{1}{A \text{ true}} u$ \mathcal{D} $\neg \neg A \text{ true}$

Proof:

Assumption u :: A true Assume $v :: \neg A$ true $\mathcal{D}_1 :: p$ true $\neg \neg A$ true by negE on u and v. by negI^{p,v} on \mathcal{D}_1 .

イロン イ部ン イヨン イヨン 三日

- Bottom-Up (backward-chaining) Consider rules that *match* the conclusion.
- Top-Down (forward-chaining) Consider rules that *matches* premisses
 - Mixed A little bottom-up, a little top-down.
 - Remark The search techniques are independent from the logic. They depend on how to *match judgments*.

伺下 イヨト イヨト

Situation Given a $\Gamma = u_1 :: \mathcal{J}_1 \dots u_n :: \mathcal{J}_n$ of hypotheses. Goal Construct evidence that \mathcal{J} is true. Remark Derived rules of inference.

$$rac{\mathcal{J}_1 \dots \mathcal{J}_n}{\mathcal{J}}$$
 derived

Subsitution Principle If $\mathcal{D}_i :: \mathcal{J}_i$ then we can construct evidence $\mathcal{D} :: \mathcal{J}$.

・ 同 ト ・ ヨ ト ・ ヨ ト



 $\frac{A \text{ true}}{\neg \neg A \text{ true}} \text{ dneg}$

is a derived rule of inference.

・回 ・ ・ ヨ ・ ・ ヨ ・

Э

Observations

- Evidence is finite.
- Subevidence relation is well-founded.
- Evidence decomposable into subevidences.

Conclusion The principle of structural induction.

高 とう ヨン うまと

Given a judgment \mathcal{J} formulated in a meta-logic. Axioms For all axioms concluding \mathcal{J} :

$$\mathcal{P}(\stackrel{}{_{\mathcal{J}}}_{\operatorname{\mathsf{J}}}\operatorname{\mathsf{axiom}})$$

Rules For all rules with premisses $\mathcal{D}_i :: \mathcal{J}_i$ concluding \mathcal{J} :

 $\mathcal{P}(\mathcal{D}_i :: \mathcal{J}_i)$ entails $\mathcal{P}(\mathcal{D} :: \mathcal{J})$

Then For all $\mathcal{D} :: \mathcal{J}, \mathcal{P}(\mathcal{D} :: \mathcal{J}).$

・吊り ・ヨリ ・ヨリー ヨ

Reasoning about logics

- Natural deduction encoded in sequent calculus. [Harper '89]
- HOL encoded in Nuprl. [Schürmann, '05]
- Isabelle/HOL encoded in HOLlight. [McLaughlin '06]
- Cut-elimination for first-order logic. [Pfenning '95, Lecture 4]
- Mechanizing the meta-theory programming languages
 - Type soundness of TAL
 - Soundness of SML
 - Compiler correctness

[Crary '03] [Crary, et al. '06] [Pfenning '92]

伺 ト イヨト イヨト

Double negation interpretation[Kolmogorov '??]Embedding of classical into intuitionistic logic.Judgment: dn(A) = B

$$dn(P) = \neg \neg P$$

$$dn(A \land B) = \neg \neg (dn(A) \land dn(B))$$

$$dn(A \lor B) = \neg \neg (dn(A) \lor dn(B))$$

$$dn(\neg A) = \neg \neg (\neg dn(A))$$

$$dn(A \supset B) = \neg \neg (dn(A) \supset dn(B))$$

白 と く ヨ と く ヨ と …

Lemma: If A ::: wff, then there exists a A' and a proof $\mathcal{D} ::: dn(A) = A'$. Proof: by structual induction on A ::: wff. Case: $A = B \land C$ $B \land C :: wff$ by assumption. B :: wff and C :: wff by inversion. B' :: wff and $\mathcal{D} :: dn(B) = B'$ by ind. hyp. on B C' :: wff and $\mathcal{E} :: dn(C) = C'$ by ind. hyp. on C $\mathcal{F} :: dn(A) = B' \land C'$ by dnand on \mathcal{D} and \mathcal{E} .

Other cases: Analogously.

向下 イヨト イヨト

Example (cont'd)

Theorem: If $\mathcal{D} :: A$ true and $\mathcal{E} :: dn(A) = A'$ then $\mathcal{F} :: A'$ true. **Proof**: by induction on \mathcal{D} :: A true Case: $\mathcal{D}_1 :: A \text{ true } \mathcal{D}_2 :: B \text{ true}$ andl $A \wedge B$ true $\mathcal{E} :: dn(A \land B) = \neg \neg (A' \land B')$ by assumption $\mathcal{E}_1 :: dn(A) = A'$ and $\mathcal{E}_2 :: dn(B) = B'$ by inversion \mathcal{F}_1 :: A' true by ind. hyp. on \mathcal{D}_1 and \mathcal{E}_1 $\mathcal{F}_2 :: B'$ true by ind. hyp. on \mathcal{D}_2 and \mathcal{E}_2 $\mathcal{F}_3 :: A' \wedge B'$ true by and I on \mathcal{F}_1 and \mathcal{F}_2 Assume $u :: \neg (A' \land B')$ \mathcal{F}_4 :: p true by negE on \mathcal{F}_3 and u $\mathcal{F} :: \neg \neg (A' \land B')$ by negl^{*p*,*u*} on \mathcal{F}_4

- 本部 ト イヨ ト - - ヨ

to show If $\mathcal{D} :: A$ true and $\mathcal{E} :: dn(A) = A'$ then $\mathcal{F} :: A'$ true. Case: $\frac{\mathcal{D}_1 :: B \land C \text{ true}}{B \text{ true}}$ and \mathbb{E}_1 $\mathcal{E} :: dn(B) = B'$ given. $\mathcal{E}_1 :: dn(C) = C'$ by Lemma above. $\mathcal{E}_2 :: dn(B \land C) = B' \land C'$ by dnand on \mathcal{E} and \mathcal{E}_1 . $\mathcal{F}_1 :: B' \land C'$ true by ind. hyp. on $\mathcal{D}_1, \mathcal{E}_2$. $\mathcal{F} :: B'$ true by inversion on \mathcal{F}_1 .

to show If $\mathcal{D} :: A$ true and $\mathcal{E} :: dn(A) = A'$ then $\mathcal{F} :: A'$ true. \overline{B} true $\begin{array}{c} U \\ \mathcal{D}_1 \\ Case: \end{array} \qquad \begin{array}{c} \mathcal{D}_1 \\ C \text{ true} \\ \overline{B \supset C} \text{ true} \end{array}$ impl HEEEEELP! We are stuck. Why?

通 と く ヨ と く ヨ と

Problem: The induction hypothesis is not general enough! It doesn't say anything about the hypotheses under which we assume that D :: A true.

Solution: Generalize the induction hypothesis.

- ► If $\mathcal{D} :: \Gamma \vdash A$ true
- ▶ and \mathcal{E} :: dn(A) = A'
- ► and for each hypothesis $u_i :: B$ true in Γ there is a hypothesis $u'_i :: B'$ true in Γ' where

$$\mathcal{E}_1$$
 :: $dn(B) = B'$

• then $\mathcal{F} :: \Gamma' \vdash A'$ true.

\$

向下 イヨト イヨト

Compatibility: Previous proofs scale!

Example (cont'd)

Case:
$$\frac{\mathcal{D}_{1} :: I, u :: B \text{ true} \vdash C \text{ true}}{\Gamma \vdash B \supset C \text{ true}} \text{ impl}^{u}$$

$$\mathcal{E} :: dn(B \supset C) = \neg \neg (B' \supset C') \text{ by assumption}$$

$$\mathcal{E}_{1} :: dn(B) = B' \text{ and } \mathcal{E}_{2} :: dn(C) = C' \text{ by inversion on } \mathcal{E}$$
Assume $p :: \text{wff}$
Assume $v :: \Gamma \vdash \neg (B' \supset C')$

$$\mathcal{F}_{1} :: \Gamma, u' :: B' \text{ true} \vdash C' \text{ true}$$

$$\mathcal{F}_{2} :: \Gamma \vdash B' \supset C' \text{ true} \text{ by impl on } \mathcal{F}_{1}$$

$$\mathcal{F}_{3} :: \Gamma \vdash p \text{ true} \text{ by negE on } v \text{ and } \mathcal{F}_{2}$$

$$\mathcal{F}_{4} :: \Gamma \vdash \neg \neg (B' \supset C') \text{ true} \text{ by negI}^{p,v} \text{ on } \mathcal{F}_{3}$$

< □ > < □ > < □ > < □ > < □ > < Ξ > < Ξ > □ Ξ

Example (cont'd)

Case: $\mathcal{D}_1 :: \Gamma, u :: A \text{ true } \vdash p \text{ true } \text{negl}^{p,u}$ $\Gamma \vdash \neg A$ true \mathcal{E} :: $dn(\neg A) = \neg \neg \neg A'$ by assumption \mathcal{E}_1 :: dn(A) = A'by inversion on \mathcal{E} Assume $q :: wff, r :: wff, v' :: \Gamma' \vdash \neg \neg A'$ $\mathcal{F}_1 :: \Gamma', u' :: A' \text{ true } \vdash \neg \neg p \text{ true}$ by ind. hyp. on \mathcal{D}_1 and \mathcal{E}_1 $\mathcal{F}_2 :: \Gamma' \cdot u' :: A' \operatorname{true} \vdash \neg \neg \neg A' \operatorname{true}$ by substitution lemma, with $\neg A'$ for $p \clubsuit$ $\mathcal{F}_3 :: \Gamma', u' :: A' \text{ true} \vdash q \text{ true}$ by negE on \mathcal{F}_2 and v'by negl^{q,u'} on \mathcal{F}_3 $\mathcal{F}_{\mathcal{A}} :: \Gamma' \vdash \neg \mathcal{A}'$ true $\mathcal{F}_{\mathsf{F}} :: \mathsf{\Gamma}' \vdash r$ true by negE on v' and \mathcal{F}_4 by negl^{r,v'} on \mathcal{F}_{F} $\mathcal{F} \cdots \Gamma' \vdash \neg \neg \neg A'$

- 4 周 ト 4 日 ト 4 日 ト - 日



Problem: We need to substitute $\neg A'$ for the hypothesis *p*:



Substitution Lemma:

- If $\mathcal{D} :: \Gamma \vdash A$ true (parametric in p)
- then $\mathcal{F} :: \Gamma \vdash [B/p](A \text{ true}).$

Proof: by structural induction on \mathcal{D} . Rest: Homework.

・ 同 ト ・ ヨ ト ・ ヨ ト

Summary

- Judgments.
- Evidence.
- Principle of structural induction.
- Inversion.
- Generalization of induction hypothesis.

Homework

- Finish the proof of cases impE, negE, orl, and orE.
- Finish the proof of the substitution lemma.

同 と く ヨ と く ヨ と …