# Natural Deduction: Making Proofs Explicit

Joshua D. Guttman

Worcester Polytechnic Institute

2 Sep 2010

# Today's Goal

Proofs are computational objects.
We want to show their computational content explicitly in our formal system.

# Conjunction Rules

$$\frac{\Gamma \vdash s : \varphi \qquad \Gamma \vdash t : \psi}{\Gamma \vdash \langle s, t \rangle : \varphi \wedge \psi}$$

$$\frac{\Gamma \vdash s : \varphi \wedge \psi}{\Gamma \vdash \mathrm{fst}(s) : \varphi} \qquad \frac{\Gamma \vdash s : \varphi \wedge \psi}{\Gamma \vdash \mathrm{scd}(s) : \psi}$$

# Axiom and Bottom

$$\frac{}{\Gamma, x : \varphi \vdash x : \varphi}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}$$

# A Derivation

$$\dfrac{\dfrac{}{x : p \wedge q \;\vdash\; x : p \wedge q}}{\dfrac{x : p \wedge q \;\vdash\; \mathsf{fst}(x) : p}{\vdash\; \text{function } x \mapsto \mathsf{fst}(x) : (p \wedge q) \to p}}$$

*We write this function:*

$$\lambda x \,.\, \mathsf{fst}(x)$$

# Lambda and Functions

- What's the derivative of $3xy^2$? $D(\lambda y \,.\, 3xy^2)$
  - With respect to $y$, its derivative is $6xy$ $= \lambda y \,.\, 6xy$
  - So if $x = 2$, that's the function $12y$ $= \lambda y \,.\, 12y$
- But: $D(\lambda x \,.\, 3xy^2)$
  - With respect to $x$, its derivative is $3y^2$ $= \lambda x \,.\, 3y^2$
  - So if $y = 3$, that's the function whose value is always 27 $= \lambda x \,.\, 27$

# A Derivation

$$\dfrac{\dfrac{\overline{x : p \wedge q \vdash x : p \wedge q}}{x : p \wedge q \vdash \mathrm{fst}(x) : p}}{\vdash \lambda x \,.\, \mathrm{fst}(x) : (p \wedge q) \to p}$$

# Implication Rules

$$\frac{\Gamma, x\colon \varphi \vdash s\colon \psi}{\Gamma \vdash \lambda x\,.\,s\colon \varphi \to \psi}$$

$$\frac{\Gamma \vdash s\colon \varphi \to \psi \qquad \Gamma \vdash t\colon \varphi}{\Gamma \vdash (st)\colon \psi}$$

# A Proof of an Implication is a Function

from proofs of the hypothesis
to proofs of the conclusion

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ d_1\\ \vdots\\ \Gamma, x:\varphi \vdash s:\psi\end{matrix}}{\Gamma \vdash \lambda x\,.\,s:\varphi\to\psi} \qquad \begin{matrix}\vdots\\ d_2\\ \vdots\\ \Gamma\vdash t:\varphi\end{matrix}}{\Gamma\vdash s[t/x]:\psi}$$

# Disjunction Rules

$$\frac{\Gamma \vdash s : \varphi}{\Gamma \vdash \langle \mathrm{lft}, s \rangle : \varphi \vee \psi} \qquad \frac{\Gamma \vdash s : \psi}{\Gamma \vdash \langle \mathrm{rgt}, s \rangle : \varphi \vee \psi}$$

$$\frac{\Gamma \vdash s : \varphi \vee \psi \qquad \Gamma, x : \varphi \vdash t : \chi \qquad \Gamma, y : \psi \vdash r : \chi}{\Gamma \vdash \mathrm{cases}(s, \lambda x \, . \, t, \lambda y \, . \, r) : \chi}$$

# Another Derivation

$$\dfrac{\dfrac{\dfrac{\overline{x : p \wedge q \;\vdash\; x : p \wedge q}}{x : p \wedge q \;\vdash\; \mathsf{fst}(x) : p}}{x : p \wedge q \;\vdash\; \langle \mathsf{lft}, \mathsf{fst}(x) \rangle : p \vee q}}{\lambda x \,.\, \langle \mathsf{lft}, \mathsf{fst}(x) \rangle : (p \wedge q) \rightarrow (p \vee q)}$$

# Axiom and Bottom

$$\frac{}{\Gamma, x : \varphi \vdash x : \varphi}$$

$$\frac{\Gamma \vdash x : \bot}{\Gamma \vdash \mathsf{emp}(x) : \varphi}$$

The Wishful Thinking Rule

# Wishful Thinking

## What about fst($x$)?

$$\dfrac{\dfrac{\dfrac{\overline{x : p \wedge q \ \vdash \ x : p \wedge q}}{x : p \wedge q \ \vdash \ \mathrm{fst}(x) : p}}{x : p \wedge q \ \vdash \ \langle \mathrm{lft}, \mathrm{fst}(x) \rangle : p \vee q}}{\lambda x \, . \, \langle \mathrm{lft}, \mathrm{fst}(x) \rangle : (p \wedge q) \rightarrow (p \vee q)}$$

This is like typechecking

# Propositions as types

- A proposition is a type
- A proof ("construction") is an object of that type
- The rules must ensure:

  If a value $s$ can be bound to a variable $x$
  and $x$ occurs in an elimination context, e.g. $\mathrm{fst}(x)$
  then $s$ permits that operation, e.g. $s = \langle t_1, t_2 \rangle$

*What are*

- *the computational rules for manipulating these objects?*
- *the properties ensured by those rules?*

# Proof objects of $\lambda_{\mathsf{ipl}}$

$$
\begin{array}{lcl}
s & ::= & v \mid \langle s, s' \rangle \\
  & \mid & \langle \mathsf{lft}, s \rangle \mid \langle \mathsf{rgt}, s \rangle \mid \lambda v \,.\, s \\
  & \mid & \mathsf{fst}(s) \mid \mathsf{scd}(s) \mid \mathsf{cases}(s, t, r) \mid ss' \\
v & ::= & x \mid \ldots
\end{array}
$$

# The Resulting Rules: Conjunction

$$\frac{\Gamma \vdash s : \varphi \qquad \Gamma \vdash t : \psi}{\Gamma \vdash \langle s, t \rangle : \varphi \wedge \psi}$$

$$\frac{\Gamma \vdash s : \varphi \wedge \psi}{\Gamma \vdash \mathrm{fst}(s) : \varphi} \qquad \frac{\Gamma \vdash s : \varphi \wedge \psi}{\Gamma \vdash \mathrm{scd}(s) : \psi}$$

# The Resulting Rules: Implication

$$\frac{\Gamma, x\colon \varphi \ \vdash \ s\colon \psi}{\Gamma \ \vdash \ \lambda x \,.\, s\colon \varphi \rightarrow \psi}$$

$$\frac{\Gamma \ \vdash \ s\colon \varphi \rightarrow \psi \qquad \Gamma \ \vdash \ t\colon \varphi}{\Gamma \ \vdash \ (st)\colon \psi}$$

# The Resulting Rules: Disjunction

$$\frac{\Gamma \vdash s : \varphi}{\Gamma \vdash \langle \mathsf{lft}, s \rangle : \varphi \vee \psi} \qquad \frac{\Gamma \vdash s : \psi}{\Gamma \vdash \langle \mathsf{rgt}, s \rangle : \varphi \vee \psi}$$

$$\frac{\Gamma \vdash s : \varphi \vee \psi \qquad \Gamma, x : \varphi \vdash t : \chi \qquad \Gamma, y : \psi \vdash r : \chi}{\Gamma \vdash \mathsf{cases}(s, \lambda x \,.\, t, \lambda y \,.\, r) : \chi}$$

# The Resulting Rules: Axiom and Falsehood

$$\frac{}{\Gamma, x : \varphi \ \vdash \ x : \varphi}$$

$$\frac{\Gamma \ \vdash \ x : \bot}{\Gamma \ \vdash \ \mathsf{emp}(x) : \varphi}$$