Proofs and Types Sums in Natural Deduction

Bow-Yaw Wang

Academia Sinica

Spring 2012

Hypothesis and Introduction Rules

- ► Hypothesis: A
- ► *Introductions*:

$$\begin{array}{ccc} \vdots & \vdots \\ \frac{A}{A} & \frac{B}{B} \end{array} \wedge \mathcal{I}$$

$$\frac{\overset{\vdots}{A}}{A \vee B} \vee 1\mathcal{I}$$

$$\frac{\vdots}{\overset{.}{B}}{A \vee B} \vee 2\mathcal{I}$$

$$\frac{\stackrel{[A]}{\vdots}}{\stackrel{B}{B}} \Rightarrow \mathcal{I}$$

$$\frac{\vdots}{\overset{\cdot}{\forall \xi. A}} \ \forall \mathcal{I}$$

$$\frac{\vdots}{\frac{A[a/\xi]}{\exists \xi.A}} \; \exists \mathcal{I}$$

▶ In $\forall \mathcal{I}$, ξ is not free in any hypothesis.

Elimination Rules

► *Eliminations*:

$$\frac{A \wedge B}{A} \wedge 1\mathcal{E} \qquad \frac{A \wedge B}{B} \wedge 2\mathcal{E} \qquad \qquad \frac{\vdots}{C} \perp \mathcal{E}$$

$$\frac{[A] \quad [B]}{\vdots \quad \vdots \quad \vdots}$$

$$\frac{A \vee B \quad C \quad C}{C} \vee \mathcal{E} \qquad \qquad \frac{A \quad A \Rightarrow B}{B} \Rightarrow$$

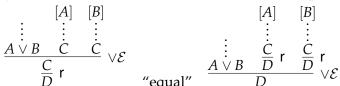
$$\vdots \qquad \vdots \qquad \vdots$$

$$\frac{\forall \xi \cdot A}{A \mid A \mid C} \forall \mathcal{E} \qquad \qquad \frac{\exists \xi \cdot A \quad C}{C} \exists \mathcal{E}$$

• ξ must not be free in the hypotheses or the conclusion after

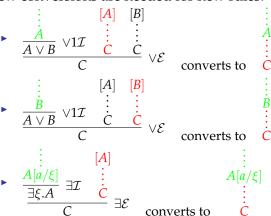
Defects

- ▶ The introduction rules $\vee 1\mathcal{I}$, $\vee 2\mathcal{I}$, and $\exists \mathcal{I}$ are nice.
 - ▶ They are symmetric to $\land 1\mathcal{E}$, $\land 2\mathcal{E}$, and $\forall \mathcal{E}$ respectively.
- ▶ The elimination rules $\bot \mathcal{E}$, $\lor \mathcal{E}$, and $\exists \mathcal{E}$ are bad.
 - ▶ They are not symmetric.
 - ▶ The formula *C* comes out of nowhere.
- ▶ They also introduce more deductions to the same "proof."



Standard Conversions

▶ New conversions are needed for new rules:



Principal Premise

Not every introduction followed by elimination is a redex. Consider

$$\begin{array}{c}
[A] \\
\vdots \\
\underline{A \Rightarrow B} \Rightarrow \mathcal{I} \quad \vdots \\
\underline{(A \Rightarrow B) \Rightarrow C} \\
C
\end{array}
\Rightarrow \mathcal{E}$$

▶ For elimination rules with multiple premises ($\Rightarrow \mathcal{E}, \lor \mathcal{E}, \exists \mathcal{E}$), a redex has an introduction ending in the *principal* premise.

- A principal branch of a deduction is a sequence of formulae A_0, A_1, \ldots, A_n that
 - $ightharpoonup A_0$ is an (undischarged) hypothesis;
 - $ightharpoonup A_n$ is the conclusion;

Subformula Property

Theorem 1

Let δ *be a normal deduction in the* $(\land, \Rightarrow, \forall)$ *fragment. Then*

- every formula in δ is a subformula of the conclusion or a hypothesis of δ ;
- if δ ends in an elimination, it has a principal branch. (particularly, the conclusion is a subformula of a hypothesis.)

Proof.

- If δ is a hypothesis, trivil.
- ▶ If δ ends in an introduction, the premises are subformulae of the conclusion. IH gives the result. For example,

$$\frac{A \qquad B}{A \wedge B} \wedge \mathcal{I}.$$

• If δ ends in an elimination, then the proof above the

Subformula Property

- For the full fragment, the subformula property does not hold.
- ▶ The "bad" eliminations can have an arbitrary *C*.
- ▶ Here is a concrete example:

Observe that two consecutive eliminations can be exchanged without changing the nature of the "proof."

$$\underbrace{ \begin{array}{ccc} [A] & [A] \\ \underline{A \wedge A} & \wedge 1 \mathcal{E} \end{array} }_{A} \underbrace{ \begin{array}{ccc} [A] & [A] \\ \underline{A \wedge A} & \wedge 1 \mathcal{E} \end{array} }_{A} \underbrace{ \begin{array}{cccc} [A] & [A] \\ \underline{A \wedge A} & \wedge 1 \mathcal{E} \end{array} }_{A} \underbrace{ \begin{array}{cccc} [A] & [A] \\ \underline{A \wedge A} & \wedge 1 \mathcal{E} \end{array} }_{A}$$

More conversions are needed!

Commuting Conversions

- $\stackrel{C}{=}$ r is an elimination of principal premise C with conclusion D.
- \triangleright Commutation of $\perp \mathcal{E}$.

$$\begin{array}{ccc}
\vdots \\
\frac{\bot}{C} \bot \mathcal{E} & \vdots \\
\hline{c} & D & r
\end{array}$$
 converts to
$$\begin{array}{ccc}
\vdots \\
\frac{\bot}{D} \bot \mathcal{E}$$

▶ Commutation of $\vee \mathcal{E}$.

Commutation of $\exists \mathcal{E}$.

[A] $\vdots \qquad \vdots$ $\exists \xi . A \qquad C$ $C \qquad \exists \mathcal{E}$

converts to $\begin{array}{c|c}
A \lor B & D \\
\hline
D \\
\vdots \\
C & \vdots \\
\hline
A \not\in A & D \\
\hline
B \not\in A
\end{array}$

Example

converts to

$$\underbrace{ \begin{bmatrix} A \end{bmatrix} \quad \begin{bmatrix} C \end{bmatrix} \quad \begin{bmatrix} D \end{bmatrix} \quad \begin{bmatrix} B \end{bmatrix} \quad \begin{bmatrix} C \end{bmatrix} \quad \begin{bmatrix} D \end{bmatrix} }_{\stackrel{\stackrel{.}{.}}{.} \stackrel{.}{.} \stackrel$$

Properties of Conversion

- ► Church-Rosser property still holds.
- ► The strong normalisation theorem also holds.
- The extension to the full fragment however is very technical
 - ▶ Just count how many rules and conversions we have!
- ▶ We will not give the details here.

- ► The full fragment has its corresponding calculus.
 - For ⊥ and ∨, we will add a new type and terms to represent deductions.
 - Observe that conversion rules for terms are derived from conversions of deductions.
- ▶ For \bot , let Emp be the *empty* type and ϵ_U : Emp $\to U$.

$$\begin{array}{ccccc} \pi^1(\epsilon_{U\times V}t) & \leadsto & \epsilon_{U}t \\ \pi^2(\epsilon_{U\times V}t) & \leadsto & \epsilon_{V}t \\ & (\epsilon_{U\to V}t)u & \leadsto & \epsilon_{V}t \\ & \epsilon_{U}(\epsilon_{\mathsf{Emp}}t) & \leadsto & \epsilon_{U}t \\ \delta x.u \ y.v \ (\epsilon_{R+S}t) & \leadsto & \epsilon_{U}t \ \end{array}$$

► For example, consider the following conversion in deductions:

$$\frac{\vdots}{\stackrel{}{\underline{U}} \Rightarrow V} \perp \mathcal{E} \quad \underline{U}}{V} \Rightarrow \mathcal{E} \quad \text{converts to} \quad \vdots \\ \downarrow \\ \overline{V} \perp \mathcal{E}$$

▶ Its corresponding conversion is

$$(\epsilon_{U\to V}t)u \leadsto \epsilon_V t$$

► For $U \lor V$, let U + V be the *sum* type, $\iota^1 : U \to U + V$ and $\iota^2 : V \to U + V$. If x : R and y : S are variables, and u : U, v : V, t : R + S are terms, then $\delta x.u \ y.v \ t : U$. The standard conversions are

$$\delta x.u \ y.v \ (\iota^1 r) \quad \rightsquigarrow \quad u[r/x] \qquad \qquad \delta x.u \ y.v \ (\iota^2 s) \quad \rightsquigarrow \quad v[s/x]$$

The commuting conversions are

► Consider the following conversion in deductions:

▶ Its corresponding conversion is

$$\epsilon_W(\delta x.u \ y.v \ t) \leadsto (\delta x.(\epsilon_W u) \ y.(\epsilon_W v) \ t)$$