Computational Logic

Interactive Theorem Proving

Week 2

Vincent van Oostrom (VvO)

March 14, 2019

Inductive definition of terms

Rule form

$$\frac{\cdot}{x^\sigma : \sigma} \qquad \frac{M : \sigma \to \tau \quad N : \sigma}{M\,N : \tau} \qquad \frac{P : \tau}{\lambda x^\sigma . P : \sigma \to \tau}$$

With a context

- Declare the free variables

$$x_1 : \sigma_1 \ \ldots, x_n : \sigma_n \vdash t : \tau$$

- Usually denoted Γ
- Derivation tree

The three typing rules with a context

Γ treated as a set: not possible for a variable to appear twice

variable rule

$$\frac{x : \sigma \in \Gamma}{\Gamma \vdash x : \sigma}$$

abstraction rule

$$\frac{\Gamma, x : \sigma \vdash P : \tau}{\Gamma \vdash (\lambda x : \sigma.\, P) : (\sigma \to \tau)}$$

application rule

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash M\, N : \tau}$$

Provability

Provability in $\lambda_{\to}$

$$\Gamma \vdash_{\lambda_{\to}} M : \sigma$$

iff there exists a derivation using the rules with the conclusion $\Gamma \vdash M : \sigma$

Formulas as Types (Curry-Howard isomorphism)

A typing judgement $M : \sigma$ can be read in two ways:

M is a function with the type σ

- term is an algorithm (program)
- type is its specification

M is a proof of the proposition σ

- type is a proposition
- term is its proof

One to one correspondence between

- Terms in $\lambda_{\rightarrow}$ (typable)
- Derivations in minimal propositional logic

Minimal Proposition Logic

Subset of Intuitionistic Propositional Logic

Only one connective: $\rightarrow$

Definition *cut*

$$\dfrac{\dfrac{\begin{array}{c}[\sigma^1]\\ \mathbb{D}_1\\ \tau\end{array}}{\sigma \rightarrow \tau}1 \qquad \begin{array}{c}\mathbb{D}_2\\ \sigma\end{array}}{\tau}$$

Minimal Proposition Logic

Subset of Intuitionistic Propositional Logic

Only one connective: $\rightarrow$

Definition *cut*-elimination

$$\dfrac{\dfrac{\dfrac{[\sigma^1]}{\mathbb{D}_1}}{\dfrac{\tau}{\sigma \rightarrow \tau}\,1} \qquad \dfrac{\mathbb{D}_2}{\sigma}}{\tau} \qquad \Longrightarrow \qquad \dfrac{\dfrac{\mathbb{D}_2}{\sigma} \qquad \dfrac{\mathbb{D}_1}{\tau}}{\tau}$$

Cut Elimination vs $\lambda_{\to}$

Lemma

Cut-elimination in minimal proposition logic corresponds to β-reduction in $\lambda_{\to}$.

$$\text{if } \mathbb{D}_1 \longrightarrow_{cut} \mathbb{D}_2 \text{ then } \mathbb{D}_1 \longrightarrow_{\beta} \mathbb{D}_2$$

Natural deduction

assumption

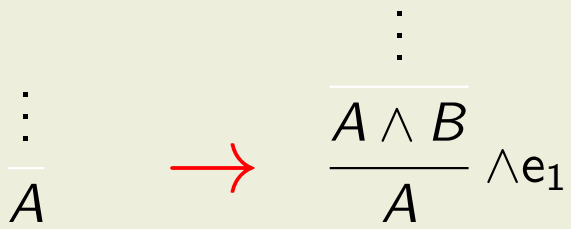
$$\frac{\vdots}{A} \quad \rightarrow \quad [A]^{\mathtt{H}}$$

conjunction introduction

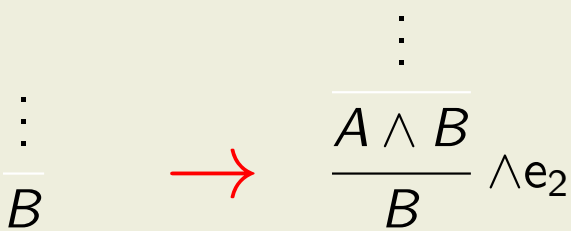
$$\frac{\vdots}{A \wedge B} \quad \rightarrow \quad \frac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{A \wedge B}\,\wedge\mathsf{i}$$

Natural deduction

conjunction elimination left



conjunction elimination right



Natural deduction

disjunction introduction left

$$\frac{\vdots}{A \vee B} \quad \rightarrow \quad \frac{\dfrac{\vdots}{A}}{A \vee B} \vee \mathrm{i}_1$$

disjunction introduction right

$$\frac{\vdots}{A \vee B} \quad \rightarrow \quad \frac{\dfrac{\vdots}{B}}{A \vee B} \vee \mathrm{i}_2$$

Natural deduction

disjunction elimination

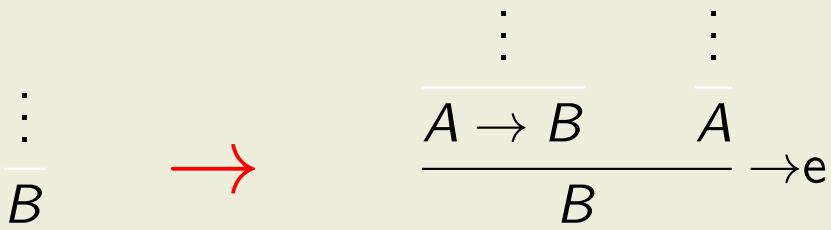
$$\dfrac{\vdots}{C} \quad \rightarrow \quad \dfrac{\begin{array}{ccc} \vdots & [A]^{\mathtt{H1}} & [B]^{\mathtt{H2}} \\ \vdots & \vdots & \vdots \\ A \vee B & C & C \end{array}}{C} \vee\mathsf{e}\,[\mathtt{H1},\mathtt{H2}]$$

implication introduction

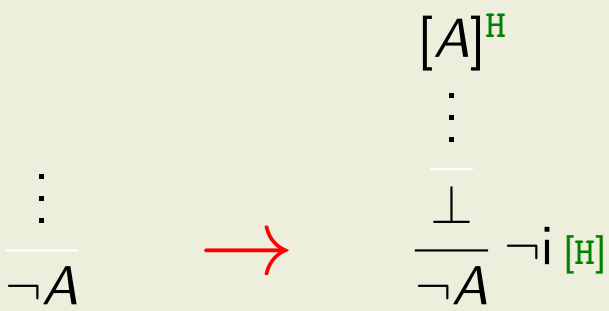
$$\dfrac{\vdots}{A \rightarrow B} \quad \rightarrow \quad \dfrac{\begin{array}{c} [A]^{\mathtt{H}} \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow\mathsf{i}\,[\mathtt{H}]$$

Natural deduction

implication elimination

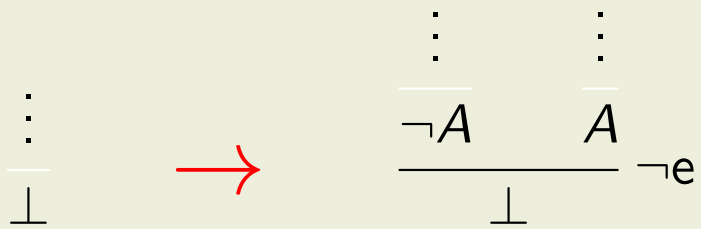


negation introduction



Natural deduction

negation elimination



bottom elimination

Natural deduction

universal introduction

$$\dfrac{\vdots}{\forall x\, A} \quad \longrightarrow \quad \dfrac{\dfrac{\vdots}{A[y/x]}}{\forall x\, A}\,\forall\mathsf{i}$$

universal elimination

$$\dfrac{\vdots}{A[t/x]} \quad \longrightarrow \quad \dfrac{\dfrac{\vdots}{\forall x\, A}}{A[t/x]}\,\forall\mathsf{e}$$

Natural deduction

existential introduction

$$\frac{\vdots}{\exists x\, A} \quad \rightarrow \quad \frac{\begin{array}{c}\vdots\\ A[t/x]\end{array}}{\exists x\, A}\,\exists\mathrm{i}$$

existential elimination

$$\frac{\vdots}{B} \quad \rightarrow \quad \frac{\exists x\, A \qquad \begin{array}{c}[A[y/x]]^{\mathrm{H}}\\ \vdots\\ B\end{array}}{B}\,\exists\mathrm{e}\,[\mathrm{H}]$$

Example Derivation

$$\dfrac{\dfrac{[\exists x(P(x) \vee \neg Q(a))]^{H1} \qquad \dfrac{[P(b) \vee \neg Q(a)]^{H3} \qquad \dfrac{[P(b)]^{H4}}{\exists x\, P(x)}\exists i \qquad \dfrac{\dfrac{[\neg Q(a)]^{H5} \quad [Q(a)]^{H2}}{\bot}\neg e}{\exists x\, P(x)}\bot e}{\exists x\, P(x)}\vee e\ [H4,H5]}{Q(a) \to \exists x\, P(x)}\exists e\ [H3]\ \to i\ [H2]}{\exists x(P(x) \vee \neg Q(a)) \to Q(a) \to \exists x\, P(x)}\to i\ [H1]$$

Corresponding Box-style Proof

1		$\exists x(P(x) \lor \neg Q(a))$	assumption
2		$Q(a)$	assumption
3	b	$P(b) \lor \neg Q(a)$	assumption
4		$P(b)$	assumption
5		$\exists x\, P(x)$	$\exists$i 4
6		$\neg Q(a)$	assumption
7		$\bot$	$\neg$e 6,2
8		$\exists x\, P(x)$	$\bot$e 7
9		$\exists x\, P(x)$	$\lor$e 3,4—5,6—8
10		$\exists x\, P(x)$	$\exists$e 1,3—9
11		$Q(a) \to \exists x\, P(x)$	$\to$i 2—10
12		$\exists x(P(x) \lor \neg Q(a)) \to Q(a) \to \exists x\, P(x)$	$\to$i 1—11

Properties of $\lambda_{\to}$

- Uniqueness of Types

$$\text{If } \Gamma \vdash M : \sigma \text{ and } \Gamma \vdash M : \tau \text{ , then } \sigma = \tau.$$

- Subject Reduction

$$\text{If } \Gamma \vdash M : \sigma \text{ and } M \to_{\beta\eta} N \text{ , then } \Gamma \vdash N : \sigma.$$

- Substitution Property

$$\text{If } \Gamma, x : \tau, \Delta \vdash M : \sigma, \Gamma \vdash P : \tau, \text{ then } \Gamma, \Delta \vdash M[x := P] : \sigma.$$

- Thinning

$$\text{If } \Gamma \vdash M : \sigma \text{ and } \Gamma \subset \Delta, \text{ then } \Delta \vdash M : \sigma.$$

- Strengthening

$$\text{If } \Gamma, x : \tau \vdash M : \sigma \text{ and } x \notin FV(M), \text{ then } \Gamma \vdash M : \sigma.$$

- Strong Normalization

$$\text{If } \Gamma \vdash M : \sigma, \text{ then all } \beta\eta\text{-reductions from } M \text{ terminate.}$$

Consequences

- Subterm property
- Condensing: $\Gamma|_{FV(M)}$
- Permutation
- No self application
- β-normal forms
- Some terms do not have fixed points

Intuitionistic Logic

Drawbacks of classical logic

- There are $x \notin \mathbb{Q}$ and $y \notin \mathbb{Q}$ st. $x^y \in \mathbb{Q}$.
  - Proof: by cases $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$
- There are seven 7s in a row in the decimal representation of π.

Brouwer, beginning of 20th century

Intuitionistic logic developed later around 1930

- $A \to \neg\neg A$ has an intuitionistic interpretation
- but $\neg\neg A \to A$ does not

Easier correspondence to $\lambda_?$-calculi

Constructive proofs have computational content

Brouwer-Heyting-Kolmogorov interpretation

Proof of $A \to B$

Function that maps proofs of A to proofs B

Proof of $A \wedge B$

Pair of proofs of A and B

Proof of $A \vee B$

Either a proof of A or a proof of B

Proof of $\forall x.P(x)$

Function that maps an object x to a proof of $P(x)$

Proof of $\bot$

Does not exist.Negation of A turns a proof of A into a non-existent object

Summary

Today

- Natural Deduction
- Properties of $\lambda \rightarrow$
- Intuitionistic Logic

Next time

- Principal Types
- Dependendent Types