

Interactive Theorem Proving

Week 3

Cezary Kaliszyk (VO)
Vincent van Oostrom (PS)

October 21, 2016



Summary

So far

Proof Assistants (history, foundations, basic properties)

HOL Light (kernel, connectives, rules)

- λ_{\rightarrow} , STT
- à la Church, à la Curry
- Type Assignment
- Curry-Howard Isomorphism and example derivations

Today

- HOL Light subgoal package
- Gentzen Style Natural Deduction
- Properties of λ_{\rightarrow}
- Principal Types
- TCP, TSP, TIP

Gentzen style natural deduction

assumption

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

conjunction introduction

$$\frac{\vdots}{A \wedge B} \rightarrow \frac{\frac{\vdots}{A} \quad \frac{\vdots}{B}}{A \wedge B} \wedge i$$

Gentzen style natural deduction

conjunction elimination left

$$\frac{\vdots}{A} \rightarrow \frac{\frac{\vdots}{A \wedge B}}{A} \wedge e_1$$

conjunction elimination right

$$\frac{\vdots}{B} \rightarrow \frac{\frac{\vdots}{A \wedge B}}{B} \wedge e_2$$

Gentzen style natural deduction

disjunction introduction left

$$\frac{\vdots}{A \vee B} \rightarrow \frac{\begin{array}{c} \vdots \\ A \end{array}}{A \vee B} \vee i_1$$

disjunction introduction right

$$\frac{\vdots}{A \vee B} \rightarrow \frac{\begin{array}{c} \vdots \\ B \end{array}}{A \vee B} \vee i_2$$

Gentzen style natural deduction

disjunction elimination

$$\frac{\begin{array}{c} \vdots \\ C \end{array} \quad \begin{array}{c} \vdots \\ A \vee B \end{array} \quad \frac{\begin{array}{c} [A]^{H1} \\ \vdots \\ C \end{array} \quad \begin{array}{c} [B]^{H2} \\ \vdots \\ C \end{array}}{C} \text{Ve } [H1, H2]}{C} \rightarrow$$

implication introduction

$$\frac{\begin{array}{c} \vdots \\ A \rightarrow B \end{array}}{A \rightarrow B} \rightarrow i [H] \quad \frac{\begin{array}{c} [A]^H \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow i [H]$$

Gentzen style natural deduction

implication elimination

$$\frac{\vdots}{B} \quad \rightarrow \quad \frac{\frac{\vdots}{A \rightarrow B} \quad \frac{\vdots}{A}}{B} \rightarrow e$$

negation introduction

$$\frac{\vdots}{\neg A} \quad \rightarrow \quad \frac{\frac{[A]^H}{\perp}}{\neg A} \neg i [H]$$

Gentzen style natural deduction

negation elimination

$$\frac{\vdots}{\perp} \quad \rightarrow \quad \frac{\frac{\vdots}{\neg A} \quad \frac{\vdots}{A}}{\perp} \neg e$$

bottom elimination

$$\frac{\vdots}{A} \quad \rightarrow \quad \frac{\frac{\vdots}{\perp}}{A} \perp e$$

Gentzen style natural deduction

universal introduction

$$\frac{\vdots}{\forall x A} \rightarrow \frac{\frac{\vdots}{A[y/x]} \forall i}{\forall x A}$$

universal elimination

$$\frac{\vdots}{A[t/x]} \rightarrow \frac{\frac{\vdots}{\forall x A}}{A[t/x]} \forall e$$

Gentzen style natural deduction

existential introduction

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

existential elimination

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

Example Derivation

$$\frac{\frac{\frac{[\exists x(P(x) \vee \neg Q(a))]^{H1}}{\exists x P(x)} \quad \frac{\frac{[P(b) \vee \neg Q(a)]^{H3}}{\exists x P(x)} \exists i \quad \frac{[P(b)]^{H4}}{\exists x P(x)} \exists i}{\exists x P(x)} \exists e [H3]}{\exists x P(x)} \exists e [H3]}{Q(a) \rightarrow \exists x P(x)} \rightarrow i [H2]}{\exists x(P(x) \vee \neg Q(a)) \rightarrow Q(a) \rightarrow \exists x P(x)} \rightarrow i [H1]$$
$$\frac{[\neg Q(a)]^{H5} \quad [Q(a)]^{H2}}{\perp} \neg e$$
$$\frac{\perp}{\exists x P(x)} \perp e$$
$$\frac{}{\exists x P(x)} \vee e [H4, H5]$$

Corresponding Box-style Proof

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

Properties of λ_{\rightarrow}

- Uniqueness of Types

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

- Subject Reduction

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

- Substitution Property

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

- Thinning

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

- Strengthening

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

- Strong Normalization

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

Consequences

- Subterm property
- Condensing: $\Gamma \upharpoonright_{FV(M)}$
- 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

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

Easier correspondence to λ -calculi

Constructive proofs have computational content

Brouwer-Heyting-Kolmogorov interpretation

Proof of $A \rightarrow B$

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 \perp

Does not exist. Negation of A turns a proof of A into a nonexistent object

Summary

Today

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

Next time

- Principal Types
- TCP, TSP, TIP
- Lambda Cube
- Polymorphism