normalization & classical logic

logical verification

week 3

2004 09 22

practical work

- monday noon is the limit
- importance of precise notation
  - labels in assumptions should go inside the brackets

    $$\begin{array}{c}[A]^x \\ \vdots\end{array} \quad \text{should be} \quad \begin{array}{c}[A^x] \\ \vdots\end{array}$$

  - left-right order of hypotheses matters

    $$\frac{\begin{array}{c}\vdots \\ A\end{array} \qquad \begin{array}{c}\vdots \\ A \to B\end{array}}{B} \quad \text{should be} \quad \frac{\begin{array}{c}\vdots \\ A \to B\end{array} \qquad \begin{array}{c}\vdots \\ A\end{array}}{B}$$

contents for today

- recap
- term & proof normalization
- variants of propositional logic

minimal logic

$\rightarrow$ introduction

$$\dfrac{\begin{array}{c}[A^x] \\ \vdots \\ B\end{array}}{A \rightarrow B}\; I[x]{\rightarrow}$$

$\rightarrow$ elimination

$$\dfrac{\begin{array}{c}\vdots \\ A \rightarrow B\end{array} \qquad \begin{array}{c}\vdots \\ A\end{array}}{B}\; E{\rightarrow}$$

$\lambda\!\to$ simply typed λ-calculus

variable rule

$$\Gamma,\, x : A,\, \Gamma' \;\vdash\; x : A$$

x does not occur in Γ'

abstraction rule

$$\frac{\Gamma,\, x : A \;\vdash\; t : B}{\Gamma \;\vdash\; (\lambda x : A.\, t) : (A \to B)}$$

application rule

$$\frac{\Gamma \;\vdash\; t : A \to B \qquad \Gamma \;\vdash\; u : A}{\Gamma \;\vdash\; t\, u : B}$$

Currying

$$A \to B \to \ (C \to D)$$

$$\lambda(x : A)\ (y : B).\ (\lambda z : C.\ M)$$

$$(f\ a\ b)\ c$$

$$A \to B \to C \to D$$

$$\lambda(x : A)\ (y : B)\ (z : C).\ M$$

$$f\ a\ b\ c$$

$$A \to (B \to (C \to D))$$

$$\lambda x : A.\ \lambda y : B.\ \lambda z : C.\ M$$

$$((f\ a)\ b)\ c$$

examples

- permutation

$$(A \to B \to C) \to (B \to A \to C)$$

- weak version of Peirce's law

$$((((A \to B) \to A) \to A) \to B) \to B$$

Curry-Howard-de Bruijn isomorphism

- **propositions as types**

  a term inhabits a type

  a proof inhabits a proposition

- **Brouwer-Heyting-Kolmogorov interpretation**

$$\lambda x : A.\, M \;:\; A \to B$$

term normalization

β-step

$$\ldots\,((\lambda x : A.\, M)\; N)\ldots \quad \rightarrow_\beta \quad \ldots\,(M[x := N])\ldots$$

$$\ldots\,((\lambda x : \mathbb{R}.\, x^2 - 2)\; 4)\ldots \quad \rightarrow_\beta \quad \ldots\,(4^2 - 2)\ldots$$

$$\ldots\,((\lambda x : A.\, x)\; y)\ldots \quad \rightarrow_\beta \quad \ldots\, y \ldots$$

substitution

renaming bound variables: α-equivalence

$$\lambda x : A.\,(\ldots\, x \ldots) \quad =_\alpha \quad \lambda y : A.\,(\ldots\, y \ldots)$$

$$\lambda x : A \to B.\,(\lambda y : A \to B.\,\lambda x : A.\,y\,x)\,x \quad \not\to_\beta \quad \lambda x : A \to B.\,(\lambda x : A.\,x\,x)$$

$$\ldots\ \lambda z : A.\,y\,z\ \ldots \quad \to_\beta \quad \lambda x : A \to B.\,(\lambda z : A.\,x\,z)$$

de Bruijn indices

$$\lambda_{A\to B}.\,(\lambda_{A\to B}.\,\lambda_A.\,1\;0)\;0 \quad \to_\beta \quad \lambda_{A\to B}.\,(\lambda_A.\,1\;0)$$

reduction

iterated beta steps

$$M_1 \ \rightarrow_\beta \ M_2 \ \rightarrow_\beta \ M_3 \ \rightarrow_\beta \ \ldots \ \rightarrow_\beta \ M_n$$

$$M_1 \ \twoheadrightarrow_\beta \ M_n$$

normal form

detours

combination of $I[\ldots]{\to}$ and $E{\to}$

$$\dfrac{\dfrac{\begin{array}{c}[A^x]\\ \vdots \\ B\end{array}}{A \to B}\; I[x]{\to} \qquad \begin{array}{c}\vdots\\ A\end{array}}{B}\; E{\to}$$

‘proof of B using a **lemma** A’

example

proof of $A \to B \to A$ with a detour

detour elimination

(cut elimination)

$$\dfrac{\dfrac{\begin{array}{c}[A^x]\\ \vdots \\ B\end{array}}{A \to B}\; I[x]{\to} \qquad \begin{array}{c}\vdots\\ A\end{array}}{B}\; E{\to} \qquad \longrightarrow \qquad \begin{array}{c}\vdots\\ A\\ \vdots\\ B\end{array}$$

Curry-Howard-De Bruijn

detour $\sim$ β-redex

β-redex: combination of abstraction and application

detour: combination of $\rightarrow$ introduction and $\rightarrow$ elimination

proof normalization	$\sim$	β-reduction
normalization step	$\sim$	reduction step
normal proof	$\sim$	normal form

proof checking & type checking

$$\overset{?}{\vdash} M : A$$

- decidable?
- complexity?

provability & inhabitation

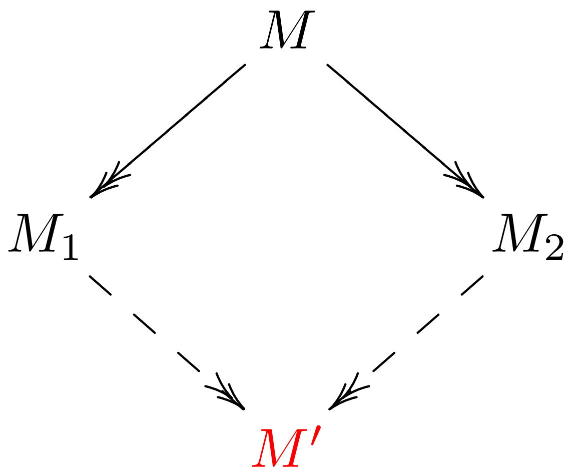
$$\vdash \ ? : A$$

- decidable?
- complexity?

consistency $\qquad \vdash \ ? : \bot$

confluence

proposition (not proved in the course)



termination

proposition (not proved in the course)

> weak termination: every term has a normal form
>
> strong termination: no term has an infinite reduction

does hold for **typed** λ-calculus

does **not** hold for untyped λ-calculus

$$(\lambda x.\, xx)\,(\lambda x.\, xx) \quad \twoheadrightarrow_\beta \quad (\lambda x.\, xx)\,(\lambda x.\, xx)$$

subject reduction

proposition (not proved in the course)

types are preserved under computation

$$\Gamma \vdash M : A \quad \& \quad M \twoheadrightarrow_\beta M' \quad \Rightarrow \quad \Gamma \vdash M' : A$$

characterization of normal forms

$$x\, N_1\, N_2\, \ldots\, N_k$$

$$\lambda x : A.\, N$$

consistency

proposition

there is no proof of $\perp$ in minimal logic

$\bot$ elimination

$$\frac{\begin{array}{c}\vdots \\ \bot\end{array}}{A}\ E\bot$$

'ex falso [sequitur] quodlibet'

```
elimtype False.
```

$\neg$ rules

negation is **defined**: $\neg A := A \to \bot$

$\neg$ introduction

$$\dfrac{\begin{matrix}[A^x]\\ \vdots \\ \bot\end{matrix}}{\neg A}\ I[x]\neg$$

$\neg$ elimination

$$\dfrac{\begin{matrix}\vdots \\ \neg A\end{matrix} \qquad \begin{matrix}\vdots \\ A\end{matrix}}{\bot}\ E\neg$$

variants of propositional logic

- minimal logic

  only implication

- minimal logic + falsum

- intuitionistic logic

  . . . + conjunction + disjunction

- classical logic

a classical proof

proposition

there are x and y such that $x \notin \mathbb{Q}$ and $y \notin \mathbb{Q}$, but $x^y \in \mathbb{Q}$

proof

$\sqrt{2} \notin \mathbb{Q}$

$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^{2} = 2 \in \mathbb{Q}$

now either $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ or $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$

in the first case $x = \sqrt{2}$ and $y = \sqrt{2}$ does the job

in the second case $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ does the job

the same proof in Mizar

```
theorem
 ex x, y st x is irrational & y is irrational & x.^.y is rational
proof
 set w = sqrt 2;
 w>0 by AXIOMS:22,SQUARE_1:84;
 then A1: (w.^.w).^.w = w.^.(w*w) by POWER:38
  .= w.^.(w^2) by SQUARE_1:def 3
  .= w.^.2 by SQUARE_1:def 4
  .= w^2 by POWER:53
  .= 2 by SQUARE_1:def 4;
 per cases;
 suppose A2: w.^.w is rational;
  take w, w;
  thus thesis by A2,Th1,INT_2:44;
 end;
 suppose A3: w.^.w is irrational;
  take w.^.w, w;
  thus thesis by A1,A3,Th1,INT_2:44;
 end;
end;
```

classical logic

- excluded middle

$$\boxed{A \vee \neg A}$$

- double negation rule

$$\neg\neg A \to A$$

- Peirce's law

$$((A \to B) \to A) \to A$$

examples of intuitionistic natural deduction

- contraposition

$$(A \to B) \to (\neg B \to \neg A)$$

- many negations

$$\neg\neg(\neg\neg A \to A)$$

examples of classical natural deduction

- using $A \vee \neg A$ one can prove

$$\neg\neg A \rightarrow A$$

- using $\neg\neg A \rightarrow A$ one can prove

$$((A \rightarrow B) \rightarrow A) \rightarrow A$$

summary

- term & proof normalization

  consistency

- variants of propositional logic

  classical logic