Type theory and logic

Lecture III: Heyting arithmetic

3 July 2014

柯向上

Department of Computer Science
University of Oxford

Hsiang-Shang.Ko@cs.ox.ac.uk

Natural numbers

- Formation:

$$\frac{}{\Gamma \;\vdash\; \mathbb{N} : \mathcal{U}}\;(\mathbb{N}\mathsf{F})$$

- Introduction:

$$\frac{}{\Gamma \;\vdash\; \mathtt{zero} : \mathbb{N}}\;(\mathbb{N}\mathsf{IZ}) \qquad \frac{\Gamma \;\vdash\; n : \mathbb{N}}{\Gamma \;\vdash\; \mathtt{suc}\; n : \mathbb{N}}\;(\mathbb{N}\mathsf{IS})$$

- Elimination:

$$\frac{\begin{array}{l}\Gamma \;\vdash\; P : \mathbb{N} \to \mathcal{U} \\ \Gamma \;\vdash\; z : P\;\mathtt{zero} \\ \Gamma \;\vdash\; s : \Pi[x : \mathbb{N}]\; P\,x \to P\,(\mathtt{suc}\; x) \\ \Gamma \;\vdash\; n : \mathbb{N}\end{array}}{\Gamma \;\vdash\; \mathtt{ind}\; P\,z\,s\,n : P\;n}\;(\mathbb{N}\mathsf{E})$$

Logically this is the *induction principle*; computationally this is *primitive recursion*.

Natural numbers — computation rules

- Computation:

$$\frac{\begin{array}{l}\Gamma \;\vdash\; P : \mathbb{N} \to \mathcal{U} \\ \Gamma \;\vdash\; z : P\,\texttt{zero} \\ \Gamma \;\vdash\; s : \Pi[x : \mathbb{N}]\; P\,x \to P\,(\texttt{suc}\;x)\end{array}}{\Gamma \;\vdash\; \texttt{ind}\;P\,z\,s\;\texttt{zero} = z \;\in\; P\;\texttt{zero}}\;(\mathbb{N}\mathrm{CZ})$$

$$\frac{\begin{array}{l}\Gamma \;\vdash\; P : \mathbb{N} \to \mathcal{U} \\ \Gamma \;\vdash\; z : P\,\texttt{zero} \\ \Gamma \;\vdash\; s : \Pi[x : \mathbb{N}]\; P\,x \to P\,(\texttt{suc}\;x) \\ \Gamma \;\vdash\; n : \mathbb{N}\end{array}}{\Gamma \;\vdash\; \texttt{ind}\;P\,z\,s\,(\texttt{suc}\;n) = s\,n\,(\texttt{ind}\;P\,z\,s\,n) \;\in\; P\,(\texttt{suc}\;n)}\;(\mathbb{N}\mathrm{CS})$$

Exercise. Define addition and multiplication with `ind`.

Induction principle

Identity types

- Formation:

$$\frac{\Gamma \vdash A : \mathcal{U} \qquad \Gamma \vdash t : A \qquad \Gamma \vdash u : A}{\Gamma \vdash \mathtt{Id}\ A\ t\ u : \mathcal{U}}\ (\equiv\mathsf{F})$$

- Introduction:

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathtt{refl}\ t : \mathtt{Id}\ A\ t\ t}\ (\equiv\mathsf{I})$$

Exercise. Assume $\Gamma \vdash t = u \in A$ and derive $\Gamma \vdash \mathtt{refl}\ t : \mathtt{Id}\ A\ t\ u$.

Identity types — elimination and computation

- Elimination:

$$\frac{\begin{array}{lll}\Gamma & \vdash & t : A \\ \Gamma & \vdash & P : \Pi[x:A]\ \mathtt{Id}\ A\ t\ x \to \mathcal{U} \\ \Gamma & \vdash & p : P\ t\ (\mathtt{refl}\ t) \\ \Gamma & \vdash & u : A \\ \Gamma & \vdash & q : \mathtt{Id}\ A\ t\ u\end{array}}{\Gamma \ \vdash\ \mathtt{J}\ P\ p\ q : P\ u\ q}\ (\equiv\mathsf{E})$$

- Computation:

$$\frac{\begin{array}{lll}\Gamma & \vdash & t : A \\ \Gamma & \vdash & P : \Pi[x:A]\ \mathtt{Id}\ A\ t\ x \to \mathcal{U} \\ \Gamma & \vdash & p : P\ t\ (\mathtt{refl}\ t)\end{array}}{\Gamma \ \vdash\ \mathtt{J}\ P\ p\ (\mathtt{refl}\ t) = p\ \in\ P\ t\ (\mathtt{refl}\ t)}\ (\equiv\mathsf{C})$$

Exercises

Exercise. Prove that `Id` is symmetric and transitive, i.e.,

$$\Pi[A:\mathcal{U}]\ \Pi[x:A]\ \Pi[y:A]\ \mathtt{Id}\ A\ x\ y \to \mathtt{Id}\ A\ y\ x$$

and

$$\begin{aligned}&\Pi[A:\mathcal{U}]\ \Pi[x:A]\ \Pi[y:A]\ \Pi[z:A]\\ &\qquad \mathtt{Id}\ A\ x\ y \to \mathtt{Id}\ A\ y\ z \to \mathtt{Id}\ A\ x\ z\end{aligned}$$

Peano axioms

Peano axioms specify an *equational theory* of natural number arithmetic; all of them are provable in type theory.

- Zero is a natural number. If *n* is a natural number, so is the successor of *n*.
  — The introduction rules.
- Equality on natural numbers is an equivalence relation; that is, it is reflexive, transitive, and symmetric.
  — We use `Id`, which indeed satisfies the above properties.
- The successor operation is an injective function, i.e.,

$$\Pi\,[\,m:\mathbb{N}\,]\ \Pi\,[\,n:\mathbb{N}\,]\ \texttt{Id}\ \mathbb{N}\ m\ n \leftrightarrow \texttt{Id}\ \mathbb{N}\ (\texttt{suc}\ m)\ (\texttt{suc}\ n)$$

- The successor operation never yields zero, i.e.,

$$\Pi\,[\,n:\mathbb{N}\,]\ \texttt{Id}\ \mathbb{N}\ (\texttt{suc}\ n)\ \texttt{zero} \to \bot$$

Peano axioms

- Addition satisfies

$$\Pi\,[\,n : \mathbb{N}\,]\ \mathtt{Id}\ \mathbb{N}\ (\mathtt{zero} + n)\ n$$

  and

$$\Pi\,[\,m : \mathbb{N}\,]\ \Pi\,[\,n : \mathbb{N}\,]\ \mathtt{Id}\ \mathbb{N}\ ((\mathtt{suc}\ m) + n)\ (\mathtt{suc}\ (m + n))$$

- Multiplication satisfies

$$\Pi\,[\,n : \mathbb{N}\,]\ \mathtt{Id}\ \mathbb{N}\ (\mathtt{zero} \times n)\ \mathtt{zero}$$

  and

$$\Pi\,[\,m : \mathbb{N}\,]\ \Pi\,[\,n : \mathbb{N}\,]\ \mathtt{Id}\ \mathbb{N}\ ((\mathtt{suc}\ m) \times n)\ (n + m \times n)$$

- The induction principle holds for natural numbers.
  — The elimination rule.