LEGO/Plastic

Julian Nagele

Interactive Theorem Proving

June 21, 2013

Outline

- Introduction
- The Theory Behind LEGO
- Demo
- Plastic

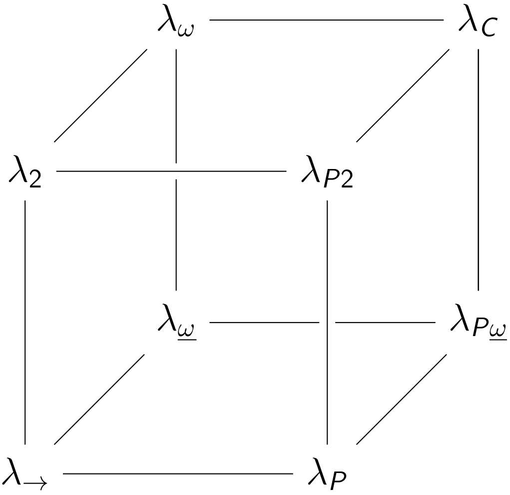
LEGO in a Nutshell

- interactive proof development system for Luo's Extended Calculus of Constructions (and related subsystems)
- refinement proof, i.e. top-down, or goal-directed proof
- Π-types: `{x:A}B`, `A->B`, λ-abstraction: `[x:A]M`, application: `(M N)`
- logical universe: `Prop`, predicative universes `Type(i)`
- was developed at University of Edinburgh by Randy Pollack in New Jersey ML
- "LEGO" was suggested by Paul Taylor to express the fun of formal constructive mathematics

The Seventeen Provers of the World

proof assistant	LEGO	Coq	HOL	Mizar	Isabelle	Agda	Minlog
de Brujin criterion	+	+	+	−	+	+	+
Poincaré principle	+	+	+	−	+	−	+
extensible by user	−	+	+	−	+	−	+
powerful automation	−	−	+	−	+	−	−
readable proof input files	−	−	−	+	+	−	−
constructive logic support	+	+	−	−	+	+	+
logical framework	−	−	−	−	+	−	−
typed	+	+	+	+	+	+	+
decidable types	+	+	+	+	+	+	+
dependent types	+	+	−	+	−	+	−
based on HO logic	+	+	+	−	+	+	−
based on ZFC set theory	−	−	−	+	+	−	−
large mathematical lib	−	+	+	+	+	−	−
statement about $\mathbb{R}$	−	+	+	+	+	−	+
statement about $\surd$	−	+	+	+	+	−	−

One More Time: λ-Cube



Pure Type Systems

- generalization of the systems in the λ-cube

Definition

pseudo-terms are defined by

$$\mathcal{T} = V \mid C \mid \mathcal{T}\mathcal{T} \mid \lambda V : \mathcal{T}.\mathcal{T} \mid \Pi V : \mathcal{T}.\mathcal{T}$$

where V and C are infinite collections of variables and constants

Definition

A PTS is a triple $\mathcal{S} = (S, A, R)$ where

- $S \subseteq C$ is a set of sorts
- $A \subseteq C \times S$ is a set of axioms
- $R \subseteq S \times S \times S$ is a set of rules

Typing Rules

AXIOM
$$\frac{c : s \in A}{\vdash c : s}$$

VAR
$$\frac{\Gamma \vdash A : s}{\Gamma, x : A \vdash x : A}$$

WEAKENING
$$\frac{\Gamma \vdash A : B \qquad \Gamma \vdash C : s}{\Gamma, x : C \vdash A : B}$$

APPLICATION
$$\frac{\Gamma \vdash M : \Pi x : A.B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B[N/x]}$$

ABSTRACTION
$$\frac{\Gamma, x : A \vdash M : B \qquad \Gamma \vdash \Pi x : A.B : s}{\Gamma \vdash \lambda x : A.M : \Pi x : A.B}$$

PRODUCT
$$\frac{(s_1, s_2, s_3) \in R \qquad \Gamma \vdash A : s_1 \qquad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash \Pi x : A.B : s_3}$$

CONVERSION
$$\frac{\Gamma \vdash A : B \qquad \Gamma \vdash B' : s \qquad B =_\beta B'}{\Gamma \vdash A : B'}$$

Examples for PTS

λ_2

$$\begin{array}{ll} S & \star, \Box \\ A & \star : \Box \\ R & (\star, \star, \star), (\Box, \star, \star) \end{array}$$

λ_C

$$\begin{array}{ll} S & \star, \Box \\ A & \star : \Box \\ R & (\star, \star, \star), (\Box, \star, \star), (\star, \Box, \Box), (\Box, \Box, \Box) \end{array}$$

$\lambda_\star$

$$\begin{array}{ll} S & \star \\ A & \star : \star \\ R & (\star, \star, \star) \end{array}$$

Theorem (Girard)

$\lambda_\star$ *is inconsistent, i.e.,* $\bot = \Pi a : \star . a$ *is inhabited*

Extended CoC

- integrates Coquand-Huet's Calculus of Constructions and Martin-Löf's type theory with universes
- an impredicative extension of Martin-Löf's type theory with universes by adding a new (impredicative) universe *Prop* of propositions
- extends the CoC by predicative type universes
- universes increase proof theoretic strength of theory (e.g. for constructive formalizations of category theory)
- needed to show that constructors of inductive types are distinct

ECC as PTS

ECC

S	$\{\star\} \cup \{\Box_i \mid i \in \mathbb{N}\}$
A	$\{\star : \Box_0\} \cup \{\Box_i : \Box_{i+1} \mid i \in \mathbb{N}\}$
R	$\{(s, \star, \star), (\star, s, s)\} \cup \{(\Box_i, \Box_j, \Box_{\max(i,j)}) \mid i, j \in \mathbb{N}\}$

- $\star$ (Prop) is impredicative: can quantify a proposition over any type
- $(\star, s, s), (\Box_i, \Box_j, \Box_{\max(i,j)})$ are predicative
- ECC also adds dependent strong Σ-types
- predicative universes $\Box_i$ are closed under Σ
- $R_\Sigma = \{(\star, s, s)\} \cup \{(\Box_i, \Box_j, \Box_{\max(i,j)}) \mid i, j \in \mathbb{N}\}$
- allowing strong Σ for impredicative universe runs into Girard's paradox

Demo

Plastic

- implementation of Typed LF
- a framework type theory to define other type theories
- may be regarded as a meta-level version of LEGO
- was implemented by Paul Callaghan in Haskell at Durham University
- "Availability: Plans to distribute Linux and Sparc executables early 2000, with source code to follow."

Summary

- Pure Type Systems generalize λ-cube
- ECC combines predicative hierarchy of universes and CoC
- LEGO is proof assistant for ECC
- Plastic is Meta-Lego

Bibliography

- Henk Barendregt, *Lambda calculi with types*, Handbook of Logic in Computer Science, vol. 2, Oxford University Press, 1991.
- Paul Callaghan and Zhaohui Luo, *An implementation of LF with coercive subtyping & universes*, JAR **27** (2001), no. 1, 3–27.
- Zhaohui Luo and Robert Pollack, *LEGO proof development system: User's manual*, Tech. report, University of Edinburgh, 1992.
- Zhaohui Luo, *An extended calculus of constructions*, Ph.D. thesis, University of Edinburgh, 1990.
- Robert Pollack, *The theory of LEGO – a proof checker for the extended calculus of constructions*, Ph.D. thesis, University of Edinburgh, 1994.