Complete Sequent Calculi for Induction and Infinite Descent

James Brotherston and Alex Simpson
Dept. of Computing, Imperial College / LFCS, University of Edinburgh

LICS-22, 10–14 July, Wroclaw, Poland

Overview

- Our interest: inductive proof principles in the setting of first-order logic with inductive definitions (FOL_{ID}).
- In this setting, the main proof techniques are:
  1. explicit rule induction over definitions;
  2. infinite descent *à la* Fermat.
- Our main goals are:
  1. to give sequent calculus proof systems for these two styles of reasoning,
  2. to justify the canonicity of our proof systems via appropriate completeness and cut-eliminability results;
  3. to investigate the relationship between the two reasoning styles.

First-order logic with inductive definitions (FOL_{ID})

- we extend standard first-order logic with a schema for inductive definitions;
- Our inductive definitions are given by a finite set Φ of *productions* each of the form:

$$\frac{P_1(\mathbf{t_1}(\mathbf{x})) \ \ldots \ P_m(\mathbf{t_m}(\mathbf{x}))}{P(\mathbf{t}(\mathbf{x}))}$$

where $P, P_1, \ldots, P_m$ are predicate symbols of the language.

Example (Natural nos; even/odd nos; transitive closure)

$$\frac{}{N0} \quad \frac{Nx}{Nsx} \qquad \frac{}{E0} \quad \frac{Ex}{Osx} \quad \frac{Ox}{Esx} \qquad \frac{Rxy}{R^+xy} \quad \frac{R^+xy \quad R^+yz}{R^+xz}$$

Standard models of FOL_{ID}

- The productions for Φ determine an n-ary monotone operator φ_Φ. E.g. for N we have:

$$\varphi_{\Phi_N}(X) = \{0^M\} \cup \{s^M x \mid x \in X\}$$

- the least prefixed point of φ_Φ can be approached via a sequence (φ_Φ^α) of approximants, obtained by iteratively applying φ_Φ to the empty set. E.g. for N we have:

$$\varphi^0_{\Phi_N} = \emptyset,\ \varphi^1_{\Phi_N} = \{0^M\},\ \varphi^2_{\Phi_N} = \{0^M, s^M 0^M\}, \ldots$$

- standard result: $\bigcup_\alpha \varphi_\Phi^\alpha$ is the least prefixed point of φ_Φ.

Definition 2.1 (Standard model)

M is a standard model if for all inductive predicates P_i we have:

$$P_i^M = \pi_i^n(\bigcup_\alpha \varphi_\Phi^\alpha) \qquad (= \pi_i^n(\varphi_\Phi^\omega))$$

Henkin models of FOL_{ID}

- we can also give non-standard interpretations to the inductive predicates of the language;
- in such models the least prefixed point of the operator for the inductive predicates is taken with respect to a specified Henkin class $\mathcal{H}$ of sets over the domain;
- Henkin classes must satisfy the property that every first-order-definable relation is interpretable in the class.

Definition 2.10 (Henkin model)

$(M, \mathcal{H})$ *is a Henkin model if the least prefixed point of* φ_Φ*, written* $\mu_\mathcal{H}.\varphi_\Phi$*, exists inside* $\mathcal{H}$ *and for all inductive predicates* P_i *we have*

$$P_i^M = \pi_i^n(\mu_\mathcal{H}.\varphi_\Phi)$$

NB. Every standard model is also a Henkin model; but there are non-standard Henkin models.

LKID: a sequent calculus for induction in FOL_{ID}

Extend the usual sequent calculus LK_e for classical first-order logic with equality by adding introduction rules for inductively defined predicates. E.g. the right-introduction rules for N are:

$$\frac{}{\Gamma \vdash N0, \Delta}\,(NR_1) \qquad \frac{\Gamma \vdash Nt, \Delta}{\Gamma \vdash Nst, \Delta}\,(NR_2)$$

The left-introduction rules embody rule induction over definitions, e.g. for N:

$$\frac{\Gamma \vdash F0, \Delta \quad \Gamma, Fx \vdash Fsx, \Delta \quad \Gamma, Ft \vdash \Delta}{\Gamma, Nt \vdash \Delta}\,(\mathrm{Ind}\ N)$$

where $x \notin FV(\Gamma \cup \Delta \cup \{Nt\})$.

NB. Mutual definitions give rise to mutual induction rules.

Results about LKID

Proposition 3.5 (Henkin soundness)

If $\Gamma \vdash \Delta$ *is provable in LKID then* $\Gamma \vdash \Delta$ *is valid with respect to Henkin models.*

Theorem 3.6 (Henkin completeness)

If $\Gamma \vdash \Delta$ *is valid with respect to Henkin models then* $\Gamma \vdash \Delta$ *has a cut-free proof in LKID.*

Corollary 3.7 (Eliminability of cut)

If $\Gamma \vdash \Delta$ *is provable in LKID then it has a cut-free proof in LKID.*

Remark. Corollary 3.7 implies the consistency of Peano arithmetic, and hence cannot itself be proven in Peano arithmetic.

$LKID^\omega$: a proof system for infinite descent in FOL_{ID}

- Rules are as for LKID except the induction rules are replaced by weaker case-split rules, e.g. for N:

$$\frac{\Gamma, t = 0 \vdash \Delta \quad \Gamma, t = sx, Nx \vdash \Delta}{\Gamma, Nt \vdash \Delta} \text{(Case } N\text{)}$$

  where $x \notin FV(\Gamma \cup \Delta \cup \{Nt\})$. We call the formula Nx in the right-hand premise a case-descendant of Nt;
- pre-proofs are infinite (non-well-founded) derivation trees;
- for soundness we need to impose a global trace condition on pre-proofs.

Traces

A trace following a path in an LKID$^\omega$ pre-proof follows an inductive predicate occurring on the left of the sequents on the path. The trace progresses when the inductive predicate is unfolded using its case-split rule. (See Defn. 4.4 in the paper for a full definition.)

Definition 4.5 (LKID$^\omega$ proof)

An LKID$^\omega$ pre-proof $\mathcal{D}$ is a proof if for every infinite path in $\mathcal{D}$ there is a trace following some tail of the path that progresses at infinitely many points.

Example

$$
\dfrac{
\dfrac{\dfrac{}{\vdash E0, O0}\,(ER_1)}{x_0 = 0 \vdash Ex_0, Ox_0}\,(\text{=L})
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{(etc.)}}{\vdots}}{Nx_1 \vdash Ex_1, Ox_1}\,(\text{Case } N)}{Nx_1 \vdash Ox_1, Osx_1}\,(OR_1)}{Nx_1 \vdash Esx_1, Osx_1}\,(ER_2)}{x_0 = sx_1, Nx_1 \vdash Ex_0, Ox_0}\,(\text{=L})
}{Nx_0 \vdash Ex_0, Ox_0}\,(\text{Case } N)
$$

Continuing the expansion of the right branch, the sequence $(Nx_0, Nx_1, \ldots, Nx_1, Nx_2, \ldots)$ is a trace along this branch with infinitely many progress points, so the pre-proof thus obtained is indeed an LKID^ω proof.

Results about $LKID^\omega$

Proposition 4.8 (Standard soundness)

If $\Gamma \vdash \Delta$ is provable in $LKID^\omega$ then $\Gamma \vdash \Delta$ is valid with respect to standard models.

Theorem 4.9 (Standard completeness)

If $\Gamma \vdash \Delta$ is valid with respect to standard models then $\Gamma \vdash \Delta$ has a cut-free proof in $LKID^\omega$.

Corollary 4.10 (Eliminability of cut)

If $\Gamma \vdash \Delta$ is provable in $LKID^\omega$ then it has a cut-free proof in $LKID^\omega$.

Remark. Unlike in LKID, cut-free proofs in LKID^ω enjoy a property akin to the subformula property, which seems close to the spirit of Girard's "purity of methods".

CLKID$^\omega$: a cyclic subsystem of LKID$^\omega$

- The infinitary system LKID$^\omega$ is unsuitable for formal reasoning — completeness with respect to standard models implies that there is no complete enumeration of LKID$^\omega$ proofs.
- However, the restriction of LKID$^\omega$ to proofs given by regular trees, which we call CLKID$^\omega$, is a natural one that *is* suitable for formal reasoning;
- in this restricted system, every proof can be represented as a finite (cyclic) graph.

Example (1)

$$
\dfrac{
  \dfrac{}{\vdash E0, O0}\;(ER_1)
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{Nz \vdash Oz, Ez\ (\dagger)}{Ny \vdash Oy, Ey}\;(\text{Subst})
      }{Ny \vdash Oy, Osy}\;(OR_1)
    }{Ny \vdash Esy, Osy}\;(ER_2)
  }{}
}{Nz \vdash Ez, Oz\ (\dagger)}\;(NL)
$$

Any infinite path necessarily has a tail consisting of repetitions of the loop indicated by $(\dagger)$, and there is a progressing trace on this loop: (Nz, Ny, Ny, Ny, Nz). By concatenating copies of this trace we obtain an infinitely progressing trace as required.

Results about $CLKID^\omega$

Proposition 6.3 (Proof-checking decidability)

It is decidable whether a $CLKID^\omega$ pre-proof is a proof.

Theorem 6.4 ($LKID \Rightarrow CLKID^\omega$)

If there is an LKID proof of $\Gamma \vdash \Delta$ then there is a $CLKID^\omega$ proof of $\Gamma \vdash \Delta$.

Conjecture 6.5 ($LKID \Leftarrow CLKID^\omega$)

If there is a $CLKID^\omega$ proof of $\Gamma \vdash \Delta$ then there is an LKID proof of $\Gamma \vdash \Delta$.

Conjecture 6.5 can be seen as a formalised version of the following assertion:

> *Proof by induction is equivalent to regular proof by infinite descent.*

Future research

- resolve the conjecture;
- investigate other applications of non-well-founded proof (cf. Alex's joint LICS/Logic Colloquium talk, Saturday);
- applications of cyclic proof to program verification (current work with Cristiano Calcagno and Richard Bornat);
- experimental implementations of cyclic proof;
- extension of our systems and results to mixed inductive and coinductive definitions.