Terminating Tableaux for the Basic Fragment of Simple Type Theory

Chad E. Brown and Gert Smolka
Saarland University

Tableaux 2009, Oslo, July 8

Decidable Higher-Order Fragments

- Propositional type theory
  - Formulas not involving individuals
  - Fixed finite model
  - Non-elementary complexity [Meyer 1974]
- MSO successor logic
  - 1 successor [Büchi 1960]
  - n successors [Rabin 1969]
  - Non-elementary complexity [Meyer 1973]
- Lambda equivalence
  - Equations between terms not involving truth values
  - Coincides with $\beta\eta$-equivalence [Friedmann 1975]
  - Non-elementary complexity [Statman 1977]
- Propositional μ-calculus [Kozen 1983]
  - ExpTime [Emerson&Jutla 1988]

Basic Formulas

1. $p(p\bot{=}p\top) = p\bot$ $\qquad p : oo$

2. $f(px) = f(p(p(px)))$ $\qquad f : o\iota, \quad x : o$

3. $x{\neq}y \land px{=}y \land py{=}x \rightarrow gp{=}g\neg$ $\qquad g : (oo)i, \quad y : o$

- Generalize quantifier-free first-order formulas
- Embedded formulas, higher-order variables
- No λ, no quantifiers, no equality for functions

Main Results

- Terminating tableau system
  deciding satisfiability of basic formulas
  - Subsystem of cut-free tableau system for full STT [B&S 2009]
  - Derived from one-sided sequent system [Brown 2004, 2007]
- Finite standard models

Definitions

- Types: $\sigma ::= o \mid \alpha \mid \sigma\sigma$
- Simply typed λ-free terms: $s ::= x \mid ss$
- Formulas: terms of type o
- Logical constants and abbreviations

$$\begin{aligned} \bot &: o \\ \to &: ooo \\ =_\alpha &: \alpha\alpha o \end{aligned}$$

$$\begin{aligned} \neg s &:= s \to \bot \\ s \neq t &:= s = t \to \bot \end{aligned}$$

Propositional Tableau System

$$\frac{\bot}{} \qquad \frac{s \to t}{\neg s \mid t} \qquad \frac{\neg(s \to t)}{s \,,\, \neg t}$$

$$\frac{x \,,\, \neg x}{}$$

- Terminates
- Complete for $x : o$

Basic Tableau Rules: Predicates

$$\frac{\bot}{}$$

$$\frac{s \rightarrow t}{\neg s \mid t}$$

$$\frac{\neg(s \rightarrow t)}{s\,,\ \neg t}$$

Mating $$\frac{x\,,\ \neg x x s_1 \ldots s_n\,,\ \neg x t_1 \ldots t_n}{s_1 {\neq} t_1 \mid \cdots \mid s_n {\neq} t_n}$$

Boolean Extensionality $$\frac{s \neq_o t}{s\,,\ \neg t \mid \neg s\,,\ t}$$

- Consider $x : o \ldots o$ (predicates on truth values)
- Mating introduces disequations between basic terms

Basic Tableau Rules: Individuals

Decomposition $\dfrac{xs_1 \ldots s_n \neq_\alpha xt_1 \ldots t_n}{s_1 \neq t_1 \mid \cdots \mid s_n \neq t_n}$

- Complete for $x : \beta \ldots \beta$ where $\beta ::= o \mid \alpha$

Basic Tableau Rules: Equality for Individuals

Confrontation $$\frac{s =_\alpha t\ ,\ u \neq_\alpha v}{s \neq u\ ,\ t \neq u \mid s \neq v\ ,\ t \neq v}$$

- New handling of equality
- Complete and terminating system for quantifier-free PL

Basic Tableau Rules: Higher-Order Variables

Functional Extensionality $\dfrac{s \neq_{\sigma\tau} t}{sx \neq tx}$ x fresh

- Sytem now complete for basic formulas

Correctness Proof

1. Refutation soundness
   - Straightforward
2. Termination
   - Lexical ordering
   - Multisets
3. Verification soundness
   - Model existence theorem
   - Maximal open branches have finite standard models

- Branch: Set of basic formulas and disequations between basic terms

Termination

- $A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots$

- Lexical ordering
  1. Progress made by FE
  2. Progress made by other rules

- Progress made by FE
  - Consider for every A_i the finite multiset that contains for every pair (s, t) of $\sigma\tau$-typed subterms of A_i the size of $\sigma\tau$, provided $\neg\exists x : (sx{\neq}tx) \in A_i$
  - Decreased by FE
  - Not increased by other rules (don't introduce subterms at function types)

Termination

- $A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots$
- Lexical ordering
  1. Progress made by FE
  2. Progress made by other rules
- Progress made by other rules
  - $\mathcal{C}A := \mathcal{S}_o A \cup \neg\mathcal{S}_o A \cup \bigcup_\sigma (\mathcal{S}_\sigma A \neq \mathcal{S}_\sigma A)$
  - $A_i \subseteq \mathcal{C}A_0$ if FE not applied
  - Size of $\mathcal{C}A$ is at most quadratic in the size of A

Model Existence Theorem

1. Let E be maximal open branch
2. Define standard frame $\mathcal{D}$
3. Define possible value relations $s \triangleright_\sigma a$
4. Show $c \triangleright \hat{\mathcal{D}}c$ for logical constants $\bot$, $\rightarrow$, $=_\alpha$
5. Show $\forall x \exists a\colon x \triangleright a$
6. Show $s, t \triangleright a \;\Rightarrow\; (s{\neq}t) \notin E$
7. Let $\mathcal{I}$ be interpretation into $\mathcal{D}$ such that $x \triangleright \mathcal{I}x$ for all x (4,5)
8. Show $s \triangleright \hat{\mathcal{I}}s$ for every basic term s
9. Show $\mathcal{I}$ satisfies E (6,8)

Definition of Standard Frame $\mathcal{D}$

- Let E be maximal open branch
- $\mathcal{D}\alpha :=$ set of all α-discriminants of E
- If $(s{\neq}t) \in E$, call s and t discriminating in E
- α-discriminant: maximal set D of discriminating terms of type α such that $\neg\exists s, t \in D\colon (s{\neq}t) \in E$
- $\mathcal{D}$ is finite if E is finite

Definition of Possible Values Relations $\triangleright_\sigma$

- Let E be maximal open branch
- Define $\triangleright_\sigma \subseteq \Lambda_\sigma \times \mathcal{D}\sigma$ by induction on types

$$
\begin{aligned}
s \triangleright_o 0 \; &:\Longleftrightarrow \; s \notin E \\
s \triangleright_o 1 \; &:\Longleftrightarrow \; \neg s \notin E \\
s \triangleright_\alpha D \; &:\Longleftrightarrow \; (s \in D \text{ if } s \text{ discriminating}) \\
s \triangleright_{\sigma\tau} f \; &:\Longleftrightarrow \; \forall t \in \Lambda_\sigma \; \forall a \in \mathcal{D}\sigma : \; t \triangleright_\sigma a \Rightarrow st \triangleright_\tau fa
\end{aligned}
$$

- Possible values relations
  - logical relations as in [Tait 1967]
  - invented for cut elimination proofs
    [Takahashi 1967, Prawitz 1967, Andrews 1971]
  - used for model construction in [Brown 2004, 2007]

Contributions

- New decidable higher-order fragment
  - finite standard models
  - NP-complete without higher-order variables
- New terminating tableau system
  - equality handled with confrontation
- New model construction
  - discriminants, standard models
- Tableau system and model construction scale to
  - EFO (basic $+ \lambda + \forall_\alpha$, $\exists_\alpha$) [TPHOLs 2009]
  - full STT
- Naive implementation beats higher-order provers
  - LEO-II, TPS, Isabelle

Future Work

- Efficient implementation as auto tactic
- Combination with congruence closure
- Complexity?
- Decidable if equations at higher types are added?