Complete Cut-Free Tableaux for Equational Simple Type Theory

Chad E. Brown and Gert Smolka
Saarland University

April 7, 2009

We present a cut-free tableau system for a version of Church's simple type theory with primitive equality. The system is formulated with an abstract normalization operator that completely hides the details of lambda conversion. We prove completeness of the system relative to Henkin models. The proof constructs Henkin models using the novel notion of a value system.

1 Introduction

Church's type theory [11] is a basic formulation of higher-order logic. Henkin [13] found a natural class of models for which Church's Hilbert-style proof system turned out to be complete. Equality, originally expressed with higher-order quantification, was later identified as the primary primitive of the theory [14, 3, 1]. In this paper we consider simple type theory with primitive equality but without descriptions or choice. We call this system ESTT for equational simple type theory. The semantics of ESTT is given by Henkin models with equality.

Modern proof theory started with Gentzen's [12] invention of a cut-free proof system for first-order logic. While Gentzen proved a cut-elimination theorem for his system, Smullyan [18] found an elegant technique (abstract consistency classes) for proving the completeness of cut-free first-order systems. Smullyan [18] found it advantageous to work with a refutation-oriented variant of Gentzen's sequent sytems [12] known as tableau systems [6, 15, 18].

The development of complete cut-free proof systems for simple type theory turned out to be hard. In 1953, Takeuti [23] introduced a sequent calculus for a lambda-free relational type theory without equality and conjectured that cut elimination holds for this system. Gentzen's [12] inductive proof of cut-elimination for first-order sequent systems does not generalize to the higher-order case since instances of formulas may be more complex than the formula itself. Moreover, Henkin's [13] completeness proof cannot be adapted for cut-free systems. Takeuti's conjecture was answered positively by Tait [20] for second-order logic, by Takahashi [21] and Prawitz [17] for higher-order logic without extensionality, and by Takahashi [22] for higher-order logic with extensionality. Building on the possible-values technique of Takahashi [21] and Prawitz [17], Takeuti [24] finally proves Henkin completeness of a cut-free sequent calculus with extensionality.

The first cut-elimination result for a calculus similar to Church's type theory was obtained by Andrews [2] in 1971. Andrews considers elementary type theory (Church's type theory without equality, extensionality, infinity, and choice) and proves that a cut-free sequent calculus is complete relative to a Hilbert-style proof system. Andrews' proof employs both the possible-values technique [21, 17] and the abstract consistency technique [18].

None of the cut-free calculi discussed above has equality as a primitive. Following Leibniz, one can define equality of a and b to hold whenever a and b satisfy the same properties. While this yields equality in standard models (full function spaces), there are Henkin models where this is not case [3]. In fact, none of the papers mentioned above contains a construction that is guarenteed to produce a Henkin model where Leibniz equality comes out as semantic equality. In addition to the model-theoretic failure, defined equality also destroys the cut-freeness of a proof system. As shown in [5] any use of Leibniz equality to say two terms are equal provides for the simulation of cut. Hence calculi that define equality as Leibniz equality cannot claim to provide cut-free equational reasoning.

The first completeness proof for a cut-free proof system relative to Henkin models with equality was given by Brown in his 2004 doctoral thesis [7] (later published as a book [8]). Brown proves the Henkin completeness of a novel one-sided sequent calculus with primitive equality. His model construction starts with Andrews' [2] non-extensional possible-values relations and then obtains a structure isomorphic to a Henkin model by taking a quotient with respect to a partial equivalence relation. Finally, abstract consistency classes [18, 2] are used to obtain the completeness result. The equality-based decomposition rules of Brown's sequent calculus have commonalities with the unification rules of the systems of Kohlhase [16] and Benzmüller [4]. Note, however, that the completeness proofs of Kohlhase and Benzmüller assume the presence of cut.

In this paper we improve and greatly simplify Brown's result [8]. For the proof system we switch to a cut-free tableau system that employs an abstract normalization operator. With the normalization operator we hide the details of lambda conversion from the tableau system and most of the completeness proof. For the completeness proof we use the new notion of a value system to directly construct surjective Henkin models. Value systems are logical relations [19] providing a relational semantics for simply-typed lambda calculus. The inspiration for value systems came from the possible-values relations used in [8, 10, 9]. In contrast to Henkin models, which obtain values for terms by induction on terms, value systems obtain values for terms by induction on types. Induction on types, which is crucial for our proofs, has the advantage of hiding the presence of the lambda binder. As a result, only a single lemma of our completeness proof deals explicitly with lambda abstractions and substitutions.

In previous work [10, 9] we study subsystems of the tableau system given in this paper and prove completeness results with respect to standard models. In [10] we show that the tableau system decides the lambda-free fragment of ESTT that restricts equations to base types. In [9] we show that the tableau system is complete with respect to standard models for the fragment of ESTT that restricts equations to base and first-order types (equations at functional types are expressed as quantified equations at base types). The normalization operator first appears in [9].

The paper is organized as follows. First we review simply typed lambda calculus and state the required properties of the normalization operator. We then introduce value systems and show how they can be used to obtain Henkin interpretations. From then on we can ignore the presence of the lambda binder. Next we introduce the type of truth values, the logical constants, the respective logical interpretations, and the tableau system. We then define evident branches as sets of normal formulas that are closed under the tableau rules and do not contain $\perp$ and prove that every evident branch has a model. The model is obtained with a value system that takes so-called discriminants [10] as basic values. Based on the notion of evidence, we then define abstract consistency and obtain the completeness result as usual. We also prove compactness and the existence of countable models.

2 Basic Definitions

We assume a countable set of **base types** (β). **Types** (σ, τ, μ) are defined inductively: (1) every base type is a type; (2) if σ and τ are types, then $\sigma\tau$ is a type. We assume a countable set of **names** (x, y), where every name comes with a unique type, and where for every type there are infinitely many names of this type. **Terms** (s, t, u, v) are defined inductively: (1) every name is a term; (2) if s is a term of type $\tau\mu$ and t is a term of type τ, then st is a term of type μ; (3) if x

is a name of type σ and t is a term of type τ, then $\lambda x.t$ is a term of type $\sigma\tau$. We write $s : \sigma$ to say that s is a term of type σ. Moreover, we write Λ_σ for the set of all terms of type σ. We assume that the set of types and the set of terms are disjoint.

A **frame** is a function $\mathcal{D}$ that maps every type to a nonempty set such that $\mathcal{D}(\sigma\tau)$ is a set of total functions from $\mathcal{D}\sigma$ to $\mathcal{D}\tau$ for all types σ, τ (i.e., $\mathcal{D}(\sigma\tau) \subseteq (\mathcal{D}\sigma \to \mathcal{D}\tau)$). An **interpretation** into a frame $\mathcal{D}$ is a function $\mathcal{I}$ that extends $\mathcal{D}$ (i.e., $\mathcal{D} \subseteq \mathcal{I}$) and maps ever name $x : \sigma$ to an element of $\mathcal{D}\sigma$ (i.e, $\mathcal{I}x \in \mathcal{D}\sigma$). If $\mathcal{I}$ is an interpretation into a frame $\mathcal{D}$, $x : \sigma$ is a name, and $a \in \mathcal{D}\sigma$, then $\mathcal{I}^x_a$ denotes the interpretation into $\mathcal{D}$ that agrees everywhere with $\mathcal{I}$ but possibly on x where it yields a. For every frame $\mathcal{D}$ we define a function $\hat{}$ that for every interpretation $\mathcal{I}$ into $\mathcal{D}$ yields a function $\hat{\mathcal{I}}$ that for some terms $s : \sigma$ returns an element of $\mathcal{D}\sigma$. The definition is by induction on terms.

$$\begin{aligned}
\hat{\mathcal{I}}x &:= \mathcal{I}x \\
\hat{\mathcal{I}}(st) &:= fa \qquad \text{if } \hat{\mathcal{I}}s = f \text{ and } \hat{\mathcal{I}}t = a \\
\hat{\mathcal{I}}(\lambda x.s) &:= f \qquad \text{if } \lambda x.s : \sigma\tau,\ f \in \mathcal{D}(\sigma\tau), \text{ and } \forall a \in \mathcal{D}\sigma\colon\ \widehat{\mathcal{I}^x_a}s = fa
\end{aligned}$$

We call $\hat{\mathcal{I}}$ the **evaluation function** of $\mathcal{I}$. A **Henkin interpretation** is an interpretation whose evaluation function is defined on all terms. An interpretation $\mathcal{I}$ is **surjective** if for every type σ and every value $a \in \mathcal{I}\sigma$ there exists a term $s : \sigma$ such that $\hat{\mathcal{I}}s = a$.

Proposition 2.1 Let $\mathcal{I}$ be a Henkin interpretation, $x : \sigma$, and $a \in \mathcal{I}\sigma$. Then $\mathcal{I}^x_a$ is a Henkin interpretation.

Proposition 2.2 If $\mathcal{I}$ is a surjective interpretation, then $\mathcal{I}\sigma$ is a countable set for every type σ.

We assume a **normalization operator** $[]$ that provides for lambda conversion. The normalization operator $[]$ must be a type preserving total function from terms to terms. We call $[s]$ the **normal form of** s and say that s is **normal** if $[s] = s$. One possible normalization operator is a function that for every term s return a β-normal term that can be obtained from s by β-reduction. We will not commit to a particular normalization operator but state explicitly the properties we require for our results. To start, we require the following properties:

N1 $[[s]] = [s]$

N2 $[[s]t] = [st]$

N3 $[xs_1 \dots s_n] = x[s_1]\dots[s_n]$ if $xs_1 \dots s_n : \beta$ and $n \geq 0$

N4 $\hat{\mathcal{I}}[s] = \hat{\mathcal{I}}s$ if $\mathcal{I}$ is a Henkin interpretation

Proposition 2.3 $xs_1 \ldots s_n : \beta$ is normal iff $s_1, \ldots, s_n$ are normal.

For the proofs of Lemma 3.3 and Theorem 3.4 we need further properties of the normalization operator that can only be expressed with substitutions. A **substitution** is a type preserving partial function from names to terms. If θ is a substitution, x is a name, and s is a term that has the same type as x, we write θ^x_s for the substitution that agrees everywhere with θ but possibly on x where it yields s. We assume that every substitution θ can be extended to a type preserving total function $\hat{\theta}$ from terms to terms such that the following conditions hold:

S1 $\hat{\theta}x = \text{if } x \in \text{Dom}\,\theta \text{ then } \theta x \text{ else } x$

S2 $\hat{\theta}(st) = (\hat{\theta}s)(\hat{\theta}t)$

S3 $[(\hat{\theta}(\lambda x.s))t] = [\widehat{\theta^x_t}s]$

S4 $[\hat{\emptyset}s] = [s]$

Note that $\emptyset$ (the empty set) is the substitution that is undefined on every name.

3 Value Systems

We introduce value systems as a tool for constructing surjective Henkin interpretations. Value systems are logical relations inspired by the possible-values relations used in [8, 10, 9].

A **value system** is a function $\rhd$ that maps every base type β to a binary relation $\rhd_\beta$ such that $\text{Dom}\,(\rhd_\beta) \subseteq \Lambda_\beta$ and $s \rhd_\beta a$ iff $[s] \rhd_\beta a$. For every value system $\rhd$ we define by induction on types:

$$\mathcal{D}\sigma := \text{Ran}\,(\rhd_\sigma)$$
$$\rhd_{\sigma\tau} := \{\, (s, f) \in \Lambda_{\sigma\tau} \times (\mathcal{D}\sigma \to \mathcal{D}\tau) \mid \forall (t, a) \in \rhd_\sigma\colon\; (st, fa) \in \rhd_\tau \,\}$$

Note that $\mathcal{D}(\sigma\tau) \subseteq (\mathcal{D}\sigma \to \mathcal{D}\tau)$ for all types $\sigma\tau$. We usually drop the type index in $s \rhd_\sigma a$ and read $s \rhd a$ as s can be a or a is a **possible value** for s.

Proposition 3.1 For every value system: $s \rhd_\sigma a$ iff $[s] \rhd_\sigma a$.

Proof By induction on σ. For base types the claim holds by the definition of value systems. Let $\sigma = \tau\mu$.

Suppose $s \rhd_{\tau\mu} a$. Let $t \rhd_\tau b$. Then $st \rhd_\mu ab$. By inductive hypothesis $[st] \rhd_\mu ab$. Thus $[[s]t] \rhd_\mu ab$ by N2. By inductive hypothesis $[s]t \rhd_\mu ab$. Hence $[s] \rhd_{\tau\mu} a$.

Suppose $[s] \rhd_{\tau\mu} a$. Let $t \rhd_\tau b$. Then $[s]t \rhd_\mu ab$. By inductive hypothesis $[[s]t] \rhd_\mu ab$. Thus $[st] \rhd_\mu ab$ by N2. By inductive hypothesis $st \rhd_\mu ab$. Hence $s \rhd_{\tau\mu} a$. ∎

A value system $\triangleright$ is **functional** if $\triangleright_\beta$ is a functional relation for every base type β.

Proposition 3.2 If $\triangleright$ is functional, then $\triangleright_\sigma$ is a functional relation for every type σ.

Proof By induction on σ. For $\sigma = \beta$, the claim is trivial. Let $\sigma = \tau\mu$ and $s \triangleright_{\tau\mu} f, g$. We show $f = g$. Let $a \in \mathcal{D}\tau$. Then $t \triangleright_\tau a$ for some t. Now $st \triangleright_\mu fa, ga$. By inductive hypothesis $fa = ga$. ■

A value system $\triangleright$ is **total** if $x \in \mathrm{Dom} \triangleright_\sigma$ for every name $x : \sigma$. An interpretation $\mathcal{I}$ is **admissible** for a value system $\triangleright$ if $\mathcal{I}\sigma = \mathcal{D}\sigma$ for all types σ and $x \triangleright \mathcal{I}x$ for all names x. Note that every total value system has admissible interpretations. We will show that admissible interpretations are Henkin interpretations that evaluate terms to possible values.

Lemma 3.3 Let $\mathcal{I}$ be an interpretation that is admissible for a value system $\triangleright$ and θ be a substitution such that $\theta x \triangleright \mathcal{I}x$ for all $x \in \mathrm{Dom}\,\theta$. Then $s \in \mathrm{Dom}\,\hat{\mathcal{I}}$ and $\hat{\theta}s \triangleright \hat{\mathcal{I}}s$ for every term s.

Proof By induction on s. Let s be a term. Case analysis.

$s = x$. The claim holds by assumption and S1.

$s = tu$. Then $t \in \mathrm{Dom}\,\hat{\mathcal{I}}$, $\hat{\theta}t \triangleright \hat{\mathcal{I}}t$, $u \in \mathrm{Dom}\,\hat{\mathcal{I}}$, and $\hat{\theta}u \triangleright \hat{\mathcal{I}}u$ by inductive hypothesis. Thus $s \in \mathrm{Dom}\,\hat{\mathcal{I}}$ and $\hat{\theta}s = (\hat{\theta}t)(\hat{\theta}u) \triangleright (\hat{\mathcal{I}}t)(\hat{\mathcal{I}}u) = \hat{\mathcal{I}}s$ using S2.

$s = \lambda x.t$ and $x : \sigma$. Let $u \triangleright_\sigma a$. We show $s \in \mathrm{Dom}\,\hat{\mathcal{I}}$ and $(\hat{\theta}s)u \triangleright (\hat{\mathcal{I}}s)a$. By inductive hypothesis we have $t \in \mathrm{Dom}\,\widehat{\mathcal{I}^x_a}$ and $\widehat{\theta^x_u}t \triangleright \widehat{\mathcal{I}^x_a}t$. Since the choice of a was unconstrained we have $s \in \mathrm{Dom}\,\hat{\mathcal{I}}$. Now $[(\hat{\theta}s)u] = [\widehat{\theta^x_u}t] \triangleright \widehat{\mathcal{I}^x_a}t = (\hat{\mathcal{I}}s)a$ using S3 and Proposition 3.1. Thus $(\hat{\theta}s)u \triangleright (\hat{\mathcal{I}}s)a$ by Proposition 3.1. ■

Theorem 3.4 Let $\mathcal{I}$ be an interpretation that is admissible for a value system $\triangleright$. Then $\mathcal{I}$ is a Henkin interpretation such that $s \triangleright \hat{\mathcal{I}}s$ for all terms s. Furthermore, $\mathcal{I}$ is surjective if $\triangleright$ is functional.

Proof Follows from Lemma 3.3 with Proposition 3.1 and S4. The second claim follows with Proposition 3.2. ■

4 Equational Simple Type Theory

We fix a base type o for the truth values and two names $\bot : o$ and $\to : ooo$ for false and implication. Moreover, we fix for every type σ a name $=_\sigma : \sigma\sigma o$ for the identity predicate for σ. An interpretation $\mathcal{I}$ is **logical** if $\mathcal{I}o = \{0, 1\}$, $\mathcal{I}\bot = 0$,

$$\mathcal{T}_{\to}\ \frac{s \to t}{\neg s \mid t} \qquad \mathcal{T}_{\neg\to}\ \frac{\neg(s \to t)}{s\,,\ \neg t}$$

$$\mathcal{T}_{\neg}\ \frac{x\,,\ \neg x}{\bot} \qquad \mathcal{T}_{\text{MAT}}\ \frac{xs_1 \dots s_n\,,\ \neg xt_1 \dots t_n}{s_1 \neq t_1 \mid \cdots \mid s_n \neq t_n}$$

$$\mathcal{T}_{\neq}\ \frac{x \neq_\alpha x}{\bot} \qquad \mathcal{T}_{\text{DEC}}\ \frac{xs_1 \dots s_n \neq_\alpha xt_1 \dots t_n}{s_1 \neq t_1 \mid \cdots \mid s_n \neq t_n}$$

$$\mathcal{T}_{\text{CON}}\ \frac{s =_\alpha t\,,\ u \neq_\alpha v}{s \neq u\,,\ t \neq u \mid s \neq v\,,\ t \neq v}$$

$$\mathcal{T}_{\text{BQ}}\ \frac{s =_o t}{s\,,\ t \ \mid\ \neg s\,,\ \neg t} \qquad \mathcal{T}_{\text{BE}}\ \frac{s \neq_o t}{s\,,\ \neg t \ \mid\ \neg s\,,\ t}$$

$$\mathcal{T}_{\text{FQ}}\ \frac{s =_{\sigma\tau} t}{[su] = [tu]}\ u \text{ normal} \qquad \mathcal{T}_{\text{FE}}\ \frac{s \neq_{\sigma\tau} t}{[sx] \neq [tx]}\ x \text{ fresh}$$

Figure 1: Tableau rules

$\mathcal{I}(\to)$ is the implication function, and $\mathcal{I}(=_\sigma)$ is the identity predicate for σ. We refer to the base types different from o as **sorts**, to the names $\bot$, $\to$ and $=_\sigma$ as **logical constants**, and to all other names as **variables**. From now on x will range over variables. Moreover, c will range over logical constants and α will range over sorts.

A **formula** is a term of type o. We employ infix notation for formulas obtained with $\to$ and $=_\sigma$ and often write **equations** $s =_\sigma t$ without the type index. We write $\top$ for $\bot \to \bot$ and $\neg s$ for $s \to \bot$. Moreover, we write $s \neq t$ for $s = t \to \bot$ and speak of a **disequation**. Note that quantified formulas $\forall x.s$ can be expressed as equations $(\lambda x.s) = (\lambda x.\top)$.

A logical Henkin interpretation $\mathcal{I}$ **satifies** a formula s if $\hat{\mathcal{I}}s = 1$. A **model** of a set of formulas A is a logical Henkin interpretation that satisfies every formula $s \in A$. A set of formulas is **satisfiable** if it has a model.

A **branch** is a set of normal formulas. The **tableau system** $\mathcal{T}$ operates on finite branches and employs the rules show in Figure 1. The side condition "x fresh" of rule $\mathcal{T}_{\text{FE}}$ requires that x does not occur in the branch the rule is applied to. We impose the following restrictions:

1. We only admit rule instances $A/A_1 \dots A_n$ where $\bot \notin A$ and $A \subsetneq A_i$ for all

$$\neg(pf \to p(\lambda x.\neg\neg fx))$$
$$pf,\ \neg p(\lambda x.\neg\neg fx)$$
$$f \neq (\lambda x.\neg\neg fx)$$
$$fx \neq \neg\neg fx$$

$fx,\ \neg\neg\neg fx$	$\neg fx,\ \neg\neg fx$
$\neg fx,\ \top$	$fx,\ \top$
$x \neq x$	$x \neq x$
$\bot$	$\bot$

Rules used: $\mathcal{T}_{\neg\to}$, $\mathcal{T}_{\text{MAT}}$, $\mathcal{T}_{\text{FE}}$, $\mathcal{T}_{\text{BE}}$, $\mathcal{T}_{\neg\to}$, $\mathcal{T}_{\text{MAT}}$, $\mathcal{T}_{\neq}$

Figure 2: Tableau refuting $\neg(pf \to p(\lambda x.\neg\neg fx))$ where $p : (\alpha o)o$ and $f : \alpha o$

$i \in \{1, \ldots, n\}$.

2. $\mathcal{T}_{\text{FE}}$ can only be applied to a disequation $(s{\neq}t) \in A$ if there is no name x such that $([sx] \neq [tx]) \in A$.

The set of **refutable branches** is defined inductively: (1) every finite branch A such that $\bot \in A$ is refutable; (2) if $A/A_1 \ldots A_n$ is an instance of a rule of $\mathcal{T}$ and $A_1, \ldots, A_n$ are refutable, then A is refutable. Figure 2 shows a refutation in $\mathcal{T}$.

A remark on the names of the rules: $\mathcal{T}_{\text{MAT}}$ is called Mating Rule, $\mathcal{T}_{\text{DEC}}$ Decomposition Rule, $\mathcal{T}_{\text{CON}}$ Confrontation Rule, $\mathcal{T}_{\text{BQ}}$ Boolean Equality Rule, $\mathcal{T}_{\text{BE}}$ Boolean Extensionality Rule, $\mathcal{T}_{\text{FQ}}$ Functional Equality Rule, and $\mathcal{T}_{\text{FE}}$ Functional Extensionality Rule.

Proposition 4.1 (Soundness) Every refutable branch is unsatisfiable.

Proof Let $A/A_1 \ldots A_n$ be an instance of a rule of $\mathcal{T}$ such that A is satisfiable. It suffices to show that one of the branches $A_1, \ldots, A_n$ is satisfiable. Straightforward. ∎

We will show that the tableau system $\mathcal{T}$ is **complete**, that is, can refute every finite unsatisfiable branch. The rules of $\mathcal{T}$ are designed such that we obtain a strong completeness result. For practical purposes one can of course strengthen $\mathcal{T}_{\neg}$ to $\frac{s,\neg s}{\bot}$ and $\mathcal{T}_{\neq}$ to $\frac{s \neq s}{\bot}$.

Every formula can be expressed by just using the identities $=_\sigma$ as logical constants [1]. If we apply the tableau rules to such formulas, disequations and negated formulas of the form $\neg x s_1 \ldots s_n$ are introduced, but no proper implications $s \to t$ where t is different from $\bot$. Hence the implication rules $\mathcal{T}_{\to}$ and $\mathcal{T}_{\neg\to}$ are not needed for branches that don't employ $\bot$ and $\to$.

$\mathcal{E}_{\perp}$	$\perp$ is not in E.
$\mathcal{E}_{\to}$	If $s \to t$ is in E, then $\neg s$ or t is in E.
$\mathcal{E}_{\neg\to}$	If $\neg(s \to t)$ is in E, then s and $\neg t$ are in E.
$\mathcal{E}_{\neg}$	If $\neg x$ is in E, then x is not in E.
$\mathcal{E}_{\mathbf{MAT}}$	If $xs_1 \dots s_n$ and $\neg xt_1 \dots t_n$ are in E where $n \ge 1$, then $s_i \ne t_i$ is in E for some $i \in \{1, \dots, n\}$.
$\mathcal{E}_{\ne}$	If $x \ne_\alpha y$ is in E, then x and y are different variables.
$\mathcal{E}_{\mathbf{DEC}}$	If $xs_1 \dots s_n \ne_\alpha xt_1 \dots t_n$ is in E where $n \ge 1$, then $s_i \ne t_i$ is in E for some $i \in \{1, \dots, n\}$.
$\mathcal{E}_{\mathbf{CON}}$	If $s =_\alpha t$ and $u \ne_\alpha v$ are in E, then either $s \ne u$ and $t \ne u$ are in E or $s \ne v$ and $t \ne v$ are in E.
$\mathcal{E}_{\mathbf{BQ}}$	If $s =_o t$ is in E, then either s and t are in E or $\neg s$ and $\neg t$ are in E.
$\mathcal{E}_{\mathbf{BE}}$	If $s \ne_o t$ is in E, then either s and $\neg t$ are in E or $\neg s$ and t are in E.
$\mathcal{E}_{\mathbf{FQ}}$	If $s =_{\sigma\tau} t$ is in E, then $[su] = [tu]$ is in E for every normal $u \in \Lambda_\sigma$.
$\mathcal{E}_{\mathbf{FE}}$	If $s \ne_{\sigma\tau} t$ is in E, then $[sx] \ne [tx]$ is in E for some variable x.

Figure 3: Evidence conditions

5 Evidence

A branch E is **evident** if it satisfies the **evidence conditions** in Figure 3. The evidence conditions correspond to the tableau rules and are designed such that every $\perp$-free branch that is closed under the tableau rules is evident. We will show that evident branches are satisfiable.

Proposition 5.1 If E is an evident branch and $\neg\neg s \in E$, then $s \in E$.

Proof Follows with $\mathcal{E}_{\neg\to}$. ∎

A branch E is **complete** if for every normal formula s either s or $\neg s$ is in E. The cut-freeness of $\mathcal{T}$ shows in the fact that there are many evident sets that are not complete. For instance, $\{pf,\ \neg p(\lambda x.\neg fx),\ f \ne \lambda x.\neg fx,\ fx \ne \neg fx,\ \neg fx\}$ is an incomplete evident branch if $p : (\sigma o)o$.

5.1 Discriminants

Given an evident branch E, we will construct a value system whose admissible logical interpretations are models of E. We start by defining the values for the sorts, which we call discriminants. Discriminants first appeared in [10].

Let E be a fixed evident branch in the following. We call a term $s : \alpha$ **discriminating** if there is some term t such that either $s \neq_\alpha t$ or $t \neq_\alpha s$ is in E. An **α-discriminant** is a maximal set a of discriminating terms of type α such that there is no disequation $s{\neq}t \in E$ such that $s, t \in a$. We write $s \sharp t$ if E contains the disequation $s{\neq}t$ or $t{\neq}s$.

Example 5.2 Suppose $E = \{x{\neq}y,\ x{\neq}z,\ y{\neq}z\}$ and $x, y, z : \alpha$. Then there are 3 α-discriminants: $\{x\}$, $\{y\}$, $\{z\}$. □

Example 5.3 Suppose $E = \{\, a_n \neq_\alpha b_n \mid n \in \mathbb{N}\,\}$ where the a_n and b_n are pairwise distinct constants. Then E is evident and there are uncountably many α-discriminants. □

Proposition 5.4 If E contains exactly n disequations at α, then there are at most 2^n α-discriminants. If E contains no disequation at α, then $\emptyset$ is the only α-discriminant.

Proposition 5.5 Let a and b be different discriminants. Then:

1. a and b are separated by a disequation in E, that is, there exist terms $s \in a$ and $t \in b$ such that $s \sharp t$.
2. a and b are not connected by an equation in E, that is, there exist no terms $s \in a$ and $t \in b$ such that $(s{=}t) \in E$.

Proof The first claim follows by contradiction. Suppose there are no terms $s \in a$ and $t \in b$ such that $s \sharp t$. Let $s \in a$. Then $s \in b$ since b is a maximal set of discriminating terms. Thus $a \subseteq b$ and hence $a = b$ since a is maximal. Contradiction.

The second claim also follows by contradiction. Suppose there is an equation $(s_1{=}s_2) \in E$ such that $s_1 \in a$ and $s_2 \in b$. By the first claim we have terms $s \in a$ and $t \in b$ such that $s \sharp t$. By $\mathcal{E}_{\mathrm{CON}}$ we have $s_1 \sharp s$ or $s_2 \sharp t$. Contradiction since a and b are discriminants. ■

5.2 Compatibility

For our proofs we need an auxiliary notion for evident branches that we call compatibility. Let E be a fixed evident branch in the following. We define relations $\|_\sigma \subseteq \Lambda_\sigma \times \Lambda_\sigma$ by induction on types:

$$s \parallel_o t \ :\Longleftrightarrow\ \{[s], \neg[t]\} \nsubseteq E \text{ and } \{\neg[s], [t]\} \nsubseteq E$$

$$s \parallel_\alpha t \ :\Longleftrightarrow\ \text{not } [s]\sharp[t]$$

$$s \parallel_{\sigma\tau} t \ :\Longleftrightarrow\ su \parallel_\tau tv \text{ whenever } u \parallel_\sigma v$$

We say that s and t are **compatible** if $s \parallel t$.

Lemma 5.6 (Compatibility)
For $n \geq 0$ and all terms s, t, $xs_1 \dots s_n$, $xt_1 \dots t_n$ of type σ:

1. Not both $s \parallel_\sigma t$ and $[s]\sharp[t]$.
2. Either $xs_1 \dots s_n \parallel_\sigma xt_1 \dots t_n$ or $[s_i]\sharp[t_i]$ for some $i \in \{1, \dots, n\}$.

Proof By induction on σ. Case analysis.

$\sigma = o$. Claim (1) follows with $\mathcal{E}_{\mathrm{BE}}$. Claim (2) follows with N3, $\mathcal{E}_{\neg}$, and $\mathcal{E}_{\mathrm{MAT}}$.

$\sigma = \alpha$. Claim (1) is trivial. Claim (2) follows with N3, $\mathcal{E}_{\neq}$, and $\mathcal{E}_{\mathrm{DEC}}$.

$\sigma = \tau\mu$. We show (1) by contradiction. Suppose $s \parallel_\sigma t$ and $[s]\sharp[t]$. By $\mathcal{E}_{\mathrm{FE}}$ $[[s]x]\sharp[[t]x]$ for some variable x. By inductive hypothesis (2) we have $x \parallel_\tau x$. Hence $sx \parallel_\mu tx$. Contradiction by inductive hypothesis (1) and N2.

To show (2), suppose $xs_1 \dots s_n \nparallel_\sigma xt_1 \dots t_n$. Then there exist terms such that $u \parallel_\tau v$ and $xs_1 \dots s_n u \nparallel_\mu xt_1 \dots t_n v$. By inductive hypothesis (1) we know that $[u]\sharp[v]$ does not hold. Hence $[s_i]\sharp[t_i]$ for some $i \in \{1, \dots, n\}$ by inductive hypothesis (2). ■

6 Model Existence

Let E be a fixed evident branch. We define a value system $\rhd$ for E:

$$s \rhd_o 0 \;:\iff\; s \in \Lambda_o \text{ and } [s] \notin E$$
$$s \rhd_o 1 \;:\iff\; s \in \Lambda_o \text{ and } \neg[s] \notin E$$
$$s \rhd_\alpha a \;:\iff\; s \in \Lambda_\alpha,\ a \text{ is an } \alpha\text{-discriminant, and } [s] \in a \text{ if } [s] \text{ is discriminating}$$

Note that N1 ensures the property $s \rhd_\beta a$ iff $[s] \rhd_\beta a$.

Proposition 6.1 $\bot \rhd_0 0$, $\top \rhd_0 1$, and $\mathcal{D}o = \{0, 1\}$.

Proof Follows with N3, $\mathcal{E}_\bot$, and Proposition 5.1. ■

Lemma 6.2 A logical interpretation is a model of E if it is admissible for $\rhd$.

Proof Let $\mathcal{I}$ be a logical interpretation that is admissible for $\rhd$, and let $s \in E$. By Theorem 3.4 we know that $\mathcal{I}$ is a Henkin interpretation and that $s \rhd_o \hat{\mathcal{I}}s$. Thus $\hat{\mathcal{I}}s \neq 0$ since $s \in E$. Hence $\hat{\mathcal{I}}s = 1$. ■

It remains to show that $\rhd$ admits logical interpretations. First we show that all sets $\mathcal{D}\sigma$ are nonempty. To do so, we prove that compatible equi-typed terms have a common value. A set T of equi-typed terms is **compatible** if $s \parallel t$ for all terms $s, t \in T$. We write $T \rhd_\sigma a$ if $T \subseteq \Lambda_\sigma$, $a \in \mathcal{D}\sigma$, and $t \rhd a$ for every $t \in T$.

Lemma 6.3 (Common Value) Let $T \subseteq \Lambda_\sigma$. Then T is compatible if and only if there exists a value a such that $T \triangleright_\sigma a$.

Proof By induction on σ.

$\sigma = \alpha$, $\Rightarrow$. Let T be compatible. Then there exists an α-discriminant a that contains all the discriminating terms in $\{ [t] \mid t \in T \}$. The claim follows since $T \triangleright a$.

$\sigma = \alpha$, $\Leftarrow$. Suppose $T \triangleright a$ and T is not compatible. Then there are terms $s, t \in T$ such that $([s]{\neq}[t]) \in E$. Thus $[s]$ and $[t]$ cannot be both in a. This contradicts $s, t \in T \triangleright a$ since $[s]$ and $[t]$ are discriminating.

$\sigma = o$, $\Rightarrow$. By contraposition. Suppose $T \not\triangleright 0$ and $T \not\triangleright 1$. Then there are terms $s, t \in T$ such that $[s], \neg[t] \in E$. Thus $s \nparallel t$. Hence T is not compatible.

$\sigma = o$, $\Leftarrow$. By contraposition. Suppose $s \nparallel_o t$ for $s, t \in T$. Then $[s], \neg[t] \in E$ without loss of generality. Hence $s \not\triangleright 0$ and $t \not\triangleright 1$. Thus $T \not\triangleright 0$ and $T \not\triangleright 1$.

$\sigma = \tau\mu$, $\Rightarrow$. Let T be compatible. We define $T_a := \{ ts \mid t \in T,\ s \triangleright_\tau a \}$ for every value $a \in \mathcal{I}\tau$ and show that T_a is compatible. Let $t_1, t_2 \in T$ and $s_1, s_2 \triangleright_\tau a$. It suffices to show $t_1 s_1 \parallel t_2 s_2$. By the inductive hypothesis $s_1 \parallel_\tau s_2$. Since T is compatible, $t_1 \parallel t_2$. Hence $t_1 s_1 \parallel t_2 s_2$.

By the inductive hypothesis we now know that for every $a \in \mathcal{I}\tau$ there is a $b \in \mathcal{I}\mu$ such that $T_a \triangleright_\mu b$. Hence there is a function $f \in \mathcal{I}\sigma$ such that $T_a \triangleright_\mu fa$ for every $a \in \mathcal{I}\tau$. Thus $T \triangleright_\sigma f$.

$\sigma = \tau\mu$, $\Leftarrow$. Let $T \triangleright_\sigma f$ and $s, t \in T$. We show $s \parallel_\sigma t$. Let $u \parallel_\tau v$. It suffices to show $su \parallel_\mu tv$. By the inductive hypothesis $u, v \triangleright_\tau a$ for some value a. Hence $su, tv \triangleright_\mu fa$. Thus $su \parallel_\mu tv$ by the inductive hypothesis. ∎

Lemma 6.4 (Admissibility) For every variable $x : \sigma$ there is some $a \in \mathcal{D}\sigma$ such that $x \triangleright a$. In particular, $\mathcal{D}\sigma$ is a nonempty set for every type σ.

Proof Let $x : \sigma$ be a variable. By Lemma 5.6 (2) we know $x \parallel_\sigma x$. Hence $\{x\}$ is compatible. By Lemma 6.3 there exists a value a such that $x \triangleright_\sigma a$. The claim follows since $a \in \mathcal{D}\sigma$ by definition of $\mathcal{D}\sigma$. ∎

Lemma 6.5 (Functionality) If $s \triangleright_\sigma a$, $t \triangleright_\sigma b$, and $(s{=}t) \in E$, then $a = b$.

Proof By contradiction and induction on σ. Assume $s \triangleright_\sigma a$, $t \triangleright_\sigma b$, $(s{=}t) \in E$, and $a \neq b$. Case analysis.

$\sigma = o$. By $\mathcal{E}_{\text{BQ}}$ either $s, t \in E$ or $\neg s, \neg t \in E$. Hence a and b are either both 1 or both 0. Contradiction.

$\sigma = \alpha$. Since $a \neq b$, there must be discriminating terms of type α. Since $(s{=}t) \in E$, we know by N3 and $\mathcal{E}_{\text{CON}}$ that s and t are normal and discriminating. Hence $s \in a$ and $t \in b$. Contradiction by Proposition 5.5 (2).

$\sigma = \tau\mu$. Since $a \neq b$, there is some $c \in \mathcal{D}\tau$ such that $ac \neq bc$. By the definition of $\mathcal{D}\tau$ and Lemma 3.1 there is a normal term u such that $u \rhd_\tau c$. Hence $su \rhd ac$ and $tu \rhd bc$. By Lemma 3.1 $[su] \rhd_\mu ac$ and $[tu] \rhd_\mu bc$. By $\mathcal{E}_{\text{FQ}}$ the equation $[su] = [tu]$ is in E. Contradiction by the inductive hypothesis. ∎

We now define the canonical interpretations for the logical constants:

$$\mathcal{L}\bot := 0$$
$$\mathcal{L}(\to) := \lambda a{\in}\mathcal{D}o.\ \lambda b{\in}\mathcal{D}o.\ \text{if } a{=}1 \text{ then } b \text{ else } 1$$
$$\mathcal{L}(=_\sigma) := \lambda a{\in}\mathcal{D}\sigma.\ \lambda b{\in}\mathcal{D}\sigma.\ \text{if } a{=}b \text{ then } 1 \text{ else } 0$$

Lemma 6.6 (Logical Constants) $c \rhd \mathcal{L}c$ for every logical constant c.

Proof $\bot \rhd \mathcal{L}\bot$ holds by $\mathcal{E}_\bot$ and N3. We show $(\to) \rhd \mathcal{L}(\to)$ by contradiction. Let $s \rhd_o a$, $t \rhd_o b$, and $(s{\to}t) \not\rhd \mathcal{L}(\to)ab$. Case analysis.

- $a = 1$ and $b = 0$. Then $\neg[s], [t] \notin E$ and $[s{\to}t] \in E$. Contradiction by N3 and $\mathcal{E}_\to$.
- $a = 0$ or $b = 1$. Then $[s] \notin E$ or $\neg[t] \notin E$, and $\neg[s{\to}t] \in E$. Contradiction by N3 and $\mathcal{E}_{\neg\to}$.

Finally, we show $(=_\sigma) \rhd \mathcal{L}(=_\sigma)$ by contradiction. Let $s \rhd_\sigma a$, $t \rhd_\sigma b$, and $(s{=_\sigma}t) \not\rhd \mathcal{L}(=_\sigma)ab$. Case analysis.

- $a = b$. Then $[s]\sharp[t]$ by N3 and $s, t \rhd a$. Thus $s \parallel t$ by Lemma 6.3. Contradiction by Lemma 5.6 (1).
- $a \neq b$. Then $([s]{=}[t]) \in E$ by N3. Hence $a = b$ by Lemmas 3.1 and 6.5. Contradiction. ∎

Theorem 6.7 (Model Existence) Every evident branch is satisfiable. Moreover, every complete evident branch has a surjective model, and every finite evident branch has a finite model.

Proof Let E be an evident branch and $\rhd$ be the value system for E. By Proposition 6.1, Lemma 6.4, and Lemma 6.6 we have a logical interpretation $\mathcal{I}$ that is admissible for $\rhd$. By Lemma 6.2 $\mathcal{I}$ is a model of E.

Let E be complete. By Theorem 3.4 we know that $\mathcal{I}$ is surjective if $\rhd$ is functional. Let $s \rhd_\beta a$ and $s \rhd_\beta b$. We show $a = b$. By Proposition 3.1 we can assume that s is normal. Thus $s{=}s$ is normal by N3. Since $\mathcal{I}$ is a model of E, we know that the formula $s{\neq}s$ is not in E. Since E is complete, we know by N3 that $s{=}s$ is in E. By Lemma 6.5 we have $a = b$.

If E is finite, $\mathcal{I}\alpha = \mathcal{D}\alpha$ is finite by Proposition 5.4. ∎

$C_\bot$	$\bot$ is not in A.
$C_\to$	If $s \to t$ is in A, then $A \cup \{\neg s\}$ or $A \cup \{t\}$ is in Γ.
$C_{\neg\to}$	If $\neg(s \to t)$ is in A, then $A \cup \{s, \neg t\}$ is in Γ.
$C_\neg$	If $\neg x$ is in A, then x is not in A.
$C_{\mathbf{MAT}}$	If $xs_1 \dots s_n$ is in A and $\neg xt_1 \dots t_n$ is in A where $n \geq 1$, then $A \cup \{s_i \neq t_i\}$ is in Γ for some $i \in \{1, \dots, n\}$.
$C_{\neq}$	If $x \neq_\alpha y$ is in A, then x and y are different variables.
$C_{\mathbf{DEC}}$	If $xs_1 \dots s_n \neq_\alpha xt_1 \dots t_n$ is in A where $n \geq 1$, then $A \cup \{s_i \neq t_i\}$ is in Γ for some $i \in \{1, \dots, n\}$.
$C_{\mathbf{CON}}$	If $s =_\alpha t$ and $u \neq_\alpha v$ are in A, then either $A \cup \{s \neq u, t \neq u\}$ or $A \cup \{s \neq v, t \neq v\}$ is in Γ.
$C_{\mathbf{BQ}}$	If $s =_o t$ is in A, then either $A \cup \{s, t\}$ or $A \cup \{\neg s, \neg t\}$ is in Γ.
$C_{\mathbf{BE}}$	If $s \neq_o t$ is in A, then either $A \cup \{s, \neg t\}$ or $A \cup \{\neg s, t\}$ is in Γ.
$C_{\mathbf{FQ}}$	If $s =_{\sigma\tau} t$ is in A, then $A \cup \{[su] \neq [tu]\}$ is in Γ for every normal $u \in \Lambda_\sigma$.
$C_{\mathbf{FE}}$	If $s \neq_{\sigma\tau} t$ is in A, then $A \cup \{[sx] \neq [tx]\}$ is in Γ for some variable x.

Figure 4: Abstract consistency conditions (must hold for every $A \in \Gamma$)

7 Abstract Consistency

We now extend the model existence result for evident branches to abstract consistency classes, following the corresponding development for first-order logic [18].

An **abstract consistency class** is a set Γ of branches such that every branch $A \in \Gamma$ satisfies the conditions in Figure 4. An abstract consistency class Γ is **complete** if for every branch $A \in \Gamma$ and every normal formula s either $A \cup \{s\}$ or $A \cup \{\neg s\}$ is in Γ.

Proposition 7.1 Let A be a branch. Then A is evident if and only if $\{A\}$ is an abstract consistency class. Moreover, A is a complete evident branch if and only if $\{A\}$ is a complete abstract consistency class.

Lemma 7.2 (Extension Lemma) Let Γ be an abstract consistency class and $A \in \Gamma$. Then there exists an evident branch E such that $A \subseteq E$. Moreover, if Γ is complete, a complete evident branch E exists such that $A \subseteq E$.

Proof Let $u_0, u_1, u_2, \ldots$ be an enumeration of all normal formulas. We construct a sequence $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$ of branches such that every $A_n \in \Gamma$. Let $A_0 := A$. We define A_{n+1} by cases. If there is no $B \in \Gamma$ such that $A_n \cup \{u_n\} \subseteq B$, then let $A_{n+1} := A_n$. Otherwise, choose some $B \in \Gamma$ such that $A_n \cup \{u_n\} \subseteq B$. We consider two subcases.

1. If u_n is of the form $s \neq_{\sigma\tau} t$, then choose A_{n+1} to be $B \cup \{[sx] \neq [tx]\} \in \Gamma$ for some variable x. This is possible since Γ satisfies C_{FE}.
2. If u_n is not of this form, then let A_{n+1} be B.

Let $E := \bigcup_{n \in \mathbb{N}} A_n$. We show that E satisfies the evidence conditions.

$\mathcal{E}_\perp$ If $\perp$ is in E, then $\perp$ is in A_n for some n, contradicting $C_\perp$.

$\mathcal{E}_\rightarrow$ Assume $s \to t$ is in E. Let n, m be such that $u_n = s$ and $u_m = t$. Let $r \geq n, m$ be such that $s \to t$ is in A_r. By $C_\rightarrow$, $A_r \cup \{\neg s\} \in \Gamma$ or $A_r \cup \{t\} \in \Gamma$. In the first case, $A_n \cup \{\neg s\} \subseteq A_r \cup \{\neg s\} \in \Gamma$, and so $\neg s \in A_{n+1} \subseteq E$. In the second case, $A_m \cup \{t\} \subseteq A_r \cup \{t\} \in \Gamma$, and so $t \in A_{m+1} \subseteq E$. Hence either $\neg s$ or t is in E.

$\mathcal{E}_{\neg\rightarrow}$ Assume $\neg(s \to t)$ is in E. Let n, m be such that $u_n = s$ and $u_m = t$. Let $r \geq n, m$ be such that $\neg(s \to t)$ is in A_r. By $C_{\neg\rightarrow}$, $A_r \cup \{s, \neg t\} \in \Gamma$. Since $A_n \cup \{s\} \subseteq A_r \cup \{s, t\}$, we have $s \in A_{n+1} \subseteq E$. Since $A_m \cup \{\neg t\} \subseteq A_r \cup \{s, t\}$, we have $\neg t \in A_{m+1} \subseteq E$.

$\mathcal{E}_\neg$ If $\neg x$ and x are in E, then $\neg x$ and x are in A_n for some n, contradicting $C_\neg$.

$\mathcal{E}_{\text{MAT}}$ Assume $xs_1 \ldots s_n$ and $\neg xt_1 \ldots t_n$ are in E for some $n \geq 1$. For each $i \in \{1, \ldots, n\}$, let m_i be such that u_{m_i} is $s_i \neq t_i$. Let $r \geq m_1, \ldots, m_n$ be such that $xs_1 \ldots s_n$ and $\neg xt_1 \ldots t_n$ are in A_r. By C_{MAT} there is some $i \in \{1, \ldots, n\}$ such that $A_r \cup \{s_i \neq t_i\} \in \Gamma$. Since $A_{m_i} \cup \{s_i \neq t_i\} \subseteq A_r \cup \{s_i \neq t_i\}$, we have $(s_i \neq t_i) \in A_{m_i+1} \subseteq E$.

$\mathcal{E}_{\neq}$ If $x \neq_\alpha x$ is in E, then $x \neq_\alpha x$ is in A_n for some n, contradicting $C_{\neq}$.

$\mathcal{E}_{\text{DEC}}$ Assume $xs_1 \ldots s_n \neq_\alpha xt_1 \ldots t_n$ is in E for some $n \geq 1$. For each $i \in \{1, \ldots, n\}$, let m_i be such that u_{m_i} is $s_i \neq t_i$. Let $r \geq m_1, \ldots, m_n$ be such that $xs_1 \ldots s_n \neq_\alpha xt_1 \ldots t_n$ is in A_r. By C_{DEC} there is some $i \in \{1, \ldots, n\}$ such that $A_r \cup \{s_i \neq t_i\} \in \Gamma$. Since $A_{m_i} \cup \{s_i \neq t_i\} \subseteq A_r \cup \{s_i \neq t_i\}$, we have $(s_i \neq t_i) \in A_{m_i+1} \subseteq E$.

$\mathcal{E}_{\text{CON}}$ Assume $s =_\alpha t$ and $u \neq_\alpha v$ are in E. Let n, m, j, k be such that u_n is $s \neq u$, u_m is $t \neq u$, u_j is $s \neq v$ and u_k is $t \neq v$. Let $r \geq n, m, j, k$ be such that $s =_\alpha t$ and $u \neq_\alpha v$ are in A_r. By C_{CON} either $A_r \cup \{s \neq u, t \neq u\}$ or $A_r \cup \{s \neq v, t \neq v\}$ is in Γ. Assume $A_r \cup \{s \neq u, t \neq u\}$ is in Γ. Since $A_n \cup \{s \neq u\} \subseteq A_r \cup \{s \neq u, t \neq u\}$, we have $s \neq u \in A_{n+1} \subseteq E$. Since $A_m \cup \{t \neq u\} \subseteq A_r \cup \{s \neq u, t \neq u\}$, we have $t \neq u \in A_{m+1} \subseteq E$. Next assume $A_r \cup \{s \neq v, t \neq v\}$ is in Γ. Since $A_j \cup \{s \neq v\} \subseteq A_r \cup \{s \neq v, t \neq v\}$, we have $s \neq v \in A_{j+1} \subseteq E$. Since $A_k \cup \{t \neq v\} \subseteq A_r \cup \{s \neq v, t \neq v\}$, we have

$t \neq v \in A_{k+1} \subseteq E$.

$\mathcal{E}_{\text{BQ}}$ Assume $s =_o t$ is in E. Let n, m, j, k be such that $u_n = s$, $u_m = t$, $u_j = \neg s$ and $u_k = \neg t$. Let $r \geq n, m, j, k$ be such that $s =_o t$ is in A_r. By $\mathcal{C}_{\text{BQ}}$ either $A_r \cup \{s, t\}$ or $A_r \cup \{\neg s, \neg t\}$ is in Γ. Assume $A_r \cup \{s, t\}$ is in Γ. Since $A_n \cup \{s\} \subseteq A_r \cup \{s, t\}$, we have $s \in E$. Since $A_m \cup \{t\} \subseteq A_r \cup \{s, t\}$, we have $t \in E$. Next assume $A_r \cup \{\neg s, \neg t\}$ is in Γ. Since $A_j \cup \{\neg s\} \subseteq A_r \cup \{\neg s, \neg t\}$, we have $\neg s \in E$. Since $A_k \cup \{\neg t\} \subseteq A_r \cup \{\neg s, \neg t\}$, we have $\neg t \in E$.

$\mathcal{E}_{\text{BE}}$ Assume $s \neq_o t$ is in E. Let n, m, j, k be such that $u_n = s$, $u_m = t$, $u_j = \neg s$ and $u_k = \neg t$. Let $r \geq n, m, j, k$ be such that $s \neq_o t$ is in A_r. By $\mathcal{C}_{\text{BE}}$ either $A_r \cup \{s, \neg t\}$ or $A_r \cup \{\neg s, t\}$ is in Γ. Assume $A_r \cup \{s, \neg t\}$ is in Γ. Since $A_n \cup \{s\} \subseteq A_r \cup \{s, \neg t\}$, we have $s \in E$. Since $A_k \cup \{\neg t\} \subseteq A_r \cup \{s, \neg t\}$, we have $\neg t \in E$. Next assume $A_r \cup \{\neg s, t\}$ is in Γ. Since $A_j \cup \{\neg s\} \subseteq A_r \cup \{\neg s, t\}$, we have $\neg s \in E$. Since $A_m \cup \{t\} \subseteq A_r \cup \{\neg s, t\}$, we have $t \in E$.

$\mathcal{E}_{\text{FQ}}$ Assume $s =_{\sigma\tau} t$ is in E and $u \in \Lambda_\sigma$ is normal. Let n be such that u_n is $[su] =_\tau [tu]$. Let $r \geq n$ be such that $s =_{\sigma\tau} t$ is in A_r. By $\mathcal{C}_{\text{FQ}}$ we know $A_r \cup \{[su] =_\tau [tu]\}$ is in Γ. Hence $[su] =_\tau [tu]$ is in A_{n+1} and also in E.

$\mathcal{E}_{\text{FE}}$ Assume $s \neq_{\sigma\tau} t$ is in E. Let n be such that u_n is $s \neq_{\sigma\tau} t$. Let $r \geq n$ be such that $s \neq_{\sigma\tau} t$ is in A_r. Since $A_n \cup \{u_n\} \subseteq A_r$, there is some variable x such that $[sx] \neq_\tau [tx]$ is in $A_{n+1} \subseteq E$.

It remains to show that E is complete if Γ is complete. Let Γ be complete and s be a normal formula. We show that s or $\neg s$ is in E. Let m, n be such that $u_m = s$ and $u_n = \neg s$. We consider $m < n$. (The case $m > n$ is symmetric.) If $s \in A_n$, we have $s \in E$. If $s \notin A_n$, then $A_n \cup \{s\}$ is not in Γ. Hence $A_n \cup \{\neg s\}$ is in Γ since Γ is complete. Hence $\neg s \in A_{n+1} \subseteq E$. ■

Theorem 7.3 (Model Existence) Every member of an abstract consistency class has a model, which is surjective if the consistency class is complete.

Proof Let $A \in \Gamma$ where Γ is an abstract consistency class. By Lemma 7.2 we have a evident set E such that $A \subseteq E$, where E is complete if Γ is complete. The claim follows with Theorem 6.7. ■

8 Completeness

It is now straightforward to prove the completeness of the tableau system $\mathcal{T}$. Let $\Gamma_{\mathcal{T}}$ be the set of all finite branches that are not refutable.

Lemma 8.1 $\Gamma_{\mathcal{T}}$ is an abstract consistency class.

Proof We have to show that $\Gamma_{\mathcal{T}}$ satisfies the abstract consistency conditions.

$C_\perp$ Suppose $\perp \in A \in \Gamma_{\mathcal{T}}$. Then A is refutable. Contradiction.

$C_\rightarrow$ Let $s \rightarrow t \in A \in \Gamma_{\mathcal{T}}$. Suppose $A \cup \{\neg s\}$ and $A \cup \{t\}$ are not in $\Gamma_{\mathcal{T}}$. Then $A \cup \{\neg s\}$ and $A \cup \{t\}$ are refutable. Hence A can be refuted using $\mathcal{T}_\rightarrow$. Contradiction.

$C_{\neg\rightarrow}$ Assume $\neg(s \rightarrow t)$ is in A and $A \cup \{s, \neg t\} \notin \Gamma_{\mathcal{T}}$. Then we can refute A using $\mathcal{T}_{\neg\rightarrow}$.

$C_\neg$ Suppose $\neg x, x \in A \in \Gamma_{\mathcal{T}}$. Then we can refute A using $\mathcal{T}_\neg$. Contradiction.

C_{MAT} Assume $\{xs_1 \dots s_n, \neg xt_1 \dots t_n\} \subseteq A$ and $A \cup \{s_i \neq t_i\} \notin \Gamma_{\mathcal{T}}$ for all $i \in \{1, \dots, n\}$. Then we can refute A using $\mathcal{T}_{\text{MAT}}$.

$C_{\neq}$ If $(x \neq_\alpha x) \in A$, then we can refute A using $\mathcal{T}_{\neq}$.

C_{DEC} Assume $xs_1 \dots s_n \neq_\alpha xt_1 \dots t_n$ is in A and $A \cup \{s_i \neq t_i\} \notin \Gamma_{\mathcal{T}}$ for all $i \in \{1, \dots, n\}$. Then we can refute A using $\mathcal{T}_{\text{DEC}}$.

C_{CON} Assume $s =_\alpha t$ and $u \neq_\alpha v$ are in A but $A \cup \{s \neq u, t \neq u\}$ and $A \cup \{s \neq v, t \neq v\}$ are not in $\Gamma_{\mathcal{T}}$. Then we can refute A using $\mathcal{T}_{\text{CON}}$.

C_{BQ} Assume $s =_o t$ is in A, $A \cup \{s, t\} \notin \Gamma_{\mathcal{T}}$ and $A \cup \{\neg s, \neg t\} \notin \Gamma_{\mathcal{T}}$. Then we can refute A using $\mathcal{T}_{\text{BQ}}$.

C_{BE} Assume $s \neq_o t$ is in A, $A \cup \{s, \neg t\} \notin \Gamma_{\mathcal{T}}$ and $A \cup \{\neg s, t\} \notin \Gamma_{\mathcal{T}}$. Then we can refute A using $\mathcal{T}_{\text{BE}}$.

C_{FQ} Let $(s =_{\sigma\tau} t) \in A \in \Gamma_{\mathcal{T}}$. Suppose $A \cup \{[su]=[tu]\} \notin \Gamma_{\mathcal{T}}$ for some normal $u \in \Lambda_\sigma$. Then $A \cup \{[su]=[tu]\}$ is refutable and so A is refutable by $\mathcal{T}_{\text{FQ}}$.

C_{FE} Let $(s \neq_{\sigma\tau} t) \in A \in \Gamma_{\mathcal{T}}$. Suppose $A \cup \{[sx] \neq [tx]\} \notin \Gamma_{\mathcal{T}}$ for every variable $x : \sigma$. Then $A \cup \{[sx] \neq [tx]\}$ is refutable for every $x : \sigma$. Hence A is refutable using $\mathcal{T}_{\text{FE}}$ and the finiteness of A. Contradiction. ∎

Theorem 8.2 (Completeness) Every unsatisfiable finite branch is refutable.

Proof By contradiction. Let A be an unsatisfiable finite branch that is not refutable. Then $A \in \Gamma_{\mathcal{T}}$ and hence A is satisfiable by Lemma 8.1 and Theorem 6.7. Contradiction. ∎

9 Compactness and Countable Models

It is known [13, 1] that equational type theory is compact and has the countable-model property. We use the opportunity and show how these properties follow with the results we already have. It is only for the existence of countable models that we make use of complete evident sets and complete abstract consistency classes.

A branch A is **sufficiently pure** if for every type σ there are infinitely many variables of type σ that do not occur in any formula of A. Let Γ_C be the set of all sufficiently pure branches A such that every finite subset of A is satisfiable. We write $\subseteq_f$ for the finite subset relation.

Lemma 9.1 Let $A \in \Gamma_C$ and $B_1, \ldots, B_n$ be finite branches such that $A \cup B_i \notin \Gamma_C$ for all $i \in \{1, \ldots, n\}$. Then there exists a finite branch $A' \subseteq_f A$ such that $A' \cup B_i$ is unsatisfiable for all $i \in \{1, \ldots, n\}$.

Proof By the assumption, we have for every $i \in \{1, \ldots, n\}$ a finite and unsatisfiable branch $C_i \subseteq A \cup B_i$. The branch $A' := (C_1 \cup \cdots \cup C_n) \cap A$ satisfies the claim. ∎

Lemma 9.2 Γ_C is a complete abstract consistency class.

Proof We verify the abstract consistency conditions using Lemma 9.1 tacitly.

$C_\perp$ We cannot have $\perp \in A$ since $\{\perp\}$ would be an unsatisfiable finite subset.

$C_\rightarrow$ Assume $s \rightarrow t$ is in A, $A \cup \{\neg s\} \notin \Gamma_C$ and $A \cup \{t\} \notin \Gamma_C$. There is some $A' \subseteq_f A$ such that $A' \cup \{\neg s\}$ and $A' \cup \{t\}$ are unsatisfiable. There is a model of $A' \cup \{s \rightarrow t\} \subseteq_f A$. This is also a model of either $A' \cup \{\neg s\}$ or $A' \cup \{t\}$, contradicting our choice of A'.

$C_{\neg\rightarrow}$ Assume $\neg(s \rightarrow t)$ is in A and $A \cup \{s, \neg t\} \notin \Gamma_C$. There is some $A' \subseteq_f A$ such that $A' \cup \{s, \neg t\}$ is unsatisfiable. There is a model of $A' \cup \{\neg(s \rightarrow t)\} \subseteq_f A$. This is also a model of $A' \cup \{s, \neg t\}$, contradicting our choice of A'.

$C_\neg$ We cannot have $\{\neg x, x\} \subseteq A$ since this would be an unsatisfiable finite subset.

C_{MAT} Assume $x s_1 \ldots s_n$ and $\neg x t_1 \ldots t_n$ are in A and $A \cup \{s_i \neq t_i\} \notin \Gamma_C$ for all $i \in \{1, \ldots, n\}$. There is some $A' \subseteq_f A$ such that $A' \cup \{s_i \neq t_i\}$ is unsatisfiable for all $i \in \{1, \ldots, n\}$. There is a model $\mathcal{I}$ of $A' \cup \{x s_1 \ldots s_n, \neg x t_1 \ldots t_n\} \subseteq_f A$. Since $\hat{\mathcal{I}}(x s_1 \ldots s_n) \neq \hat{\mathcal{I}}(x t_1 \ldots t_n)$, we must have $\hat{\mathcal{I}}(s_i) \neq \hat{\mathcal{I}}(t_i)$ for some $i \in \{1, \ldots, n\}$. Thus $\mathcal{I}$ models $A' \cup \{s_i \neq t_i\}$, contradicting our choice of A'.

$C_{\neq}$ We cannot have $(x \neq_\alpha x) \in A$ since $\{x \neq x\}$ would be an unsatisfiable finite subset.

C_{DEC} Assume $x s_1 \ldots s_n \neq_\alpha x t_1 \ldots t_n$ is in A and $A \cup \{s_i \neq t_i\} \notin \Gamma_C$ for all $i \in \{1, \ldots, n\}$. There is some $A' \subseteq_f A$ such that $A' \cup \{s_i \neq t_i\}$ is unsatisfiable for all $i \in \{1, \ldots, n\}$. There is a model $\mathcal{I}$ of $A' \cup \{x s_1 \ldots s_n \neq_\alpha x t_1 \ldots t_n\} \subseteq_f A$. Since $\hat{\mathcal{I}}(x s_1 \ldots s_n) \neq \hat{\mathcal{I}}(x t_1 \ldots t_n)$, we must have $\hat{\mathcal{I}}(s_i) \neq \hat{\mathcal{I}}(t_i)$ for some $i \in \{1, \ldots, n\}$. Thus $\mathcal{I}$ models $A' \cup \{s_i \neq t_i\}$, contradicting our choice of A'.

C_{CON} Assume $s =_\alpha t$ and $u \neq_\alpha v$ are in A, $A \cup \{s \neq u, t \neq u\} \notin \Gamma_C$ and $A \cup \{s \neq v, t \neq v\} \notin \Gamma_C$. There is some $A' \subseteq_f A$ such that $A' \cup \{s \neq u, t \neq$

$u\}$ and $A' \cup \{s \neq v, t \neq v\}$ are unsatisfiable. There is a model $\mathcal{I}$ of $A' \cup \{s = t, u \neq v\} \subseteq_f A$. Since $\hat{\mathcal{I}}(s) = \hat{\mathcal{I}}(t)$ and $\hat{\mathcal{I}}(u) \neq \hat{\mathcal{I}}(v)$, we either have $\hat{\mathcal{I}}(s) \neq \hat{\mathcal{I}}(u)$ and $\hat{\mathcal{I}}(t) \neq \hat{\mathcal{I}}(u)$ or $\hat{\mathcal{I}}(s) \neq \hat{\mathcal{I}}(v)$ and $\hat{\mathcal{I}}(t) \neq \hat{\mathcal{I}}(v)$. Hence $\mathcal{I}$ models either $A' \cup \{s \neq u, t \neq u\}$ and $A' \cup \{s \neq v, t \neq v\}$, contradicting our choice of A'.

$\mathcal{C}_{\text{BQ}}$ Assume $s =_o t$ is in A, $A \cup \{s, t\} \notin \Gamma_{\text{C}}$ and $A \cup \{\neg s, \neg t\} \notin \Gamma_{\text{C}}$. There is some $A' \subseteq_f A$ such that $A' \cup \{s, t\}$ and $A' \cup \{\neg s, \neg t\}$ are unsatisfiable. There is a model of $A' \cup \{s =_o t\} \subseteq_f A$. This is also a model of $A' \cup \{s, t\}$ or $A' \cup \{\neg s, \neg t\}$.

$\mathcal{C}_{\text{BE}}$ Assume $s \neq_o t$ is in A, $A \cup \{s, \neg t\} \notin \Gamma_{\text{C}}$ and $A \cup \{\neg s, t\} \notin \Gamma_{\text{C}}$. There is some $A' \subseteq_f A$ such that $A' \cup \{s, \neg t\}$ and $A' \cup \{\neg s, t\}$ are unsatisfiable. There is a model of $A' \cup \{s \neq_o t\} \subseteq_f A$. This is also a model of $A' \cup \{s, \neg t\}$ or $A' \cup \{\neg s, t\}$.

$\mathcal{C}_{\text{FQ}}$ Assume $s =_{\sigma\tau} t$ is in A but $A \cup \{[su] =_\tau [tu]\}$ is not in Γ_{C} for some normal $u \in \Lambda_\sigma$. There is some $A' \subseteq_f A$ such that $A' \cup \{[su] = [tu]\}$ is unsatisfiable. There is a model $\mathcal{I}$ of $A' \cup \{s = t\} \subseteq_f A$. Since $\hat{\mathcal{I}}(s) = \hat{\mathcal{I}}(t)$, we know $\hat{\mathcal{I}}([su]) = \hat{\mathcal{I}}(su) = \hat{\mathcal{I}}(s)\hat{\mathcal{I}}(u) = \hat{\mathcal{I}}(t)\hat{\mathcal{I}}(u) = \hat{\mathcal{I}}(tu) = \hat{\mathcal{I}}([tu])$ using N4. Hence $\mathcal{I}$ is a model of $A' \cup \{[su] = [tu]\}$, a contradiction.

$\mathcal{C}_{\text{FE}}$ Assume $s \neq_{\sigma\tau} t$ is in A. Since A is sufficiently pure, there is a variable $x : \sigma$ which does not occur in A. Assume $A \cup \{[sx] \neq [tx]\} \notin \Gamma_{\text{C}}$. There is some $A' \subseteq_f A$ such that $A' \cup \{[sx] \neq [tx]\}$ is unsatisfiable. There is a model $\mathcal{I}$ of $A' \cup \{s \neq t\} \subseteq_f A$. Since $\hat{\mathcal{I}}(s) \neq \hat{\mathcal{I}}(t)$, there must be some $a \in \mathcal{I}\sigma$ such that $\hat{\mathcal{I}}(s)a \neq \hat{\mathcal{I}}(t)a$. Since x does not occur in A, we know $\widehat{\mathcal{I}_a^x}(sx) \neq \widehat{\mathcal{I}_a^x}(tx)$ and $\mathcal{I}_a^x$ is a model of A'. Since $\widehat{\mathcal{I}_a^x}([sx]) = \widehat{\mathcal{I}_a^x}(sx)$ by N4 and $\widehat{\mathcal{I}_a^x}([tx]) = \widehat{\mathcal{I}_a^x}(tx)$, we conclude $\mathcal{I}_a^x$ is a model of $A' \cup \{[sx] \neq [tx]\}$, contradicting our choice of A'.

We show the completeness of Γ_{C} by contradiction. Let $A \in \Gamma_{\text{C}}$ and s be a normal formula such that $A \cup \{s\}$ and $A \cup \{\neg s\}$ are not in Γ_{C}. Then there exists $A' \subseteq_f A$ such that $A' \cup \{s\}$ and $A' \cup \{\neg s\}$ are unsatisfiable. Contradiction since A' is satisfiable. ■

Theorem 9.3 Let A be a branch such that every finite subset of A is satisfiable. Then A has a countable model.

Proof Without loss of generality we assume A is sufficiently pure. Then $A \in \Gamma_{\text{C}}$. Hence A has a countable model by Lemma 9.2 and Theorem 7.3. ■

10 Conclusion

Equational simple type theory (ESTT) is an elegant and expressive generalization of first-order logic. Like first-order logic, ESTT comes with a natural notion of model for which complete deduction systems exist. Unfortunately, the proof theory of ESTT is not well developed. A cut-free alternative to the Hilbert system of Andrews [1] only appeared in 2004 [7]. In this paper we formulate the sequent system of [7] as a cut-free tableau system and give a much simplified completeness proof. Our main innovation are the notions of value system and abstract normalization operator.

References

[1] P. B. Andrews. *An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof*. Kluwer Academic Publishers, 2nd edition, 2002.

[2] Peter B. Andrews. Resolution in type theory. *J. Symb. Log.*, 36:414–432, 1971.

[3] Peter B. Andrews. General models and extensionality. *J. Symb. Log.*, 37:395–397, 1972.

[4] Christoph Benzmüller. Extensional higher-order paramodulation and RUE-resolution. In *Proc. of CADE*, volume 1632 of *LNAI*, pages 399–413. Springer, 1999.

[5] Christoph Benzmüller, Chad E. Brown, and Michael Kohlhase. Cut-simulation and impredicativity. *Logical Methods in Computer Science*, 5(1):1–21, 2009.

[6] Evert W. Beth. Semantic entailment and formal derivability. *Mededelingen der Koninklijke Nederlandse Akademie van Wetenschappen, Afdeling Letterkunde*, 18(13):309–342, 1955.

[7] Chad E. Brown. *Set Comprehension in Church's Type Theory*. PhD thesis, Department of Mathematical Sciences, Carnegie Mellon University, 2004.

[8] Chad E. Brown. *Automated Reasoning in Higher-Order Logic: Set Comprehension and Extensionality in Church's Type Theory*. College Publications, 2007.

[9] Chad E. Brown and Gert Smolka. Extended first-order logic. Technical report, Programming Systems Lab, Saarland University, March 2009. Submitted.

[10] Chad E. Brown and Gert Smolka. Terminating tableaux for the basic fragment of simple type theory. In *Tableaux 2009*, LNCS. Springer, 2009. To appear.

[11] Alonzo Church. A formulation of the simple theory of types. *J. Symb. Log.*, 5:56–68, 1940.

[12] Gerhard Gentzen. Untersuchungen über das natürliche Schließen I, II. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935.

[13] Leon Henkin. Completeness in the theory of types. *J. Symb. Log.*, 15:81–91, 1950.

[14] Leon Henkin. A theory of propositional types. *Fundamenta Mathematicae*, 52:323–344, 1963.

[15] K. Jaakko J. Hintikka. Form and content in quantification theory. Two papers on symbolic logic. *Acta Philosophica Fennica*, 8:7–55, 1955.

[16] Michael Kohlhase. Higher-order tableaux. In Peter Baumgartner, Reiner Hähnle, and Joachim Posegga, editors, *TABLEAUX*, volume 918 of *LNCS*, pages 294–309. Springer, 1995.

[17] Dag Prawitz. Hauptsatz for higher order logic. *J. Symb. Log.*, 33:452–457, 1968.

[18] Raymond M. Smullyan. *First-Order Logic*. Springer, 1968.

[19] Richard Statman. Logical relations and the typed λ-calculus. *Information and Control*, 65:85–97, 1985.

[20] William W. Tait. A nonconstructive proof of Gentzen's Hauptsatz for second order predicate logic. *Bulletin of the American Math. Society*, 72(6):980–983, 1966.

[21] Moto-o Takahashi. A proof of cut-elimination theorem in simple type theory. *Journal of the Mathematical Society of Japan*, 19:399–410, 1967.

[22] Moto-o Takahashi. Simple Type Theory of Gentzen Style with the Inference of Extensionality. *Proc. Japan Acad.*, 44:43–45, 1968.

[23] Gaisi Takeuti. On a generalized logic calculus. *Japanese Journal of Mathematics*, 23:39–96, 1953. Errata: ibid, vol. 24 (1954), 149–156.

[24] Gaisi Takeuti. *Proof Theory*. Elsevier Science Publishers, 1975.