

Extended First-Order Logic

Chad E. Brown and Gert Smolka
Saarland University

June 5, 2009

We consider the EFO fragment of simple type theory, which restricts quantification and equality to base types but retains lambda abstractions and higher-order variables. We show that this fragment enjoys the characteristic properties of first-order logic: complete proof systems, compactness, and countable models. We obtain these results with an analytic tableau system and a concomitant model existence lemma. All results are with respect to standard models. The tableau system is well-suited for proof search and yields decision procedures for substantial fragments of EFO.

1 Introduction

First-order logic can be considered as a natural fragment of Church's type theory [1]. In this paper we exhibit a larger fragment of type theory, called EFO, that still enjoys the characteristic properties of first-order logic: complete proof systems, compactness, and countable models. EFO restricts quantification and equality to base types but retains lambda abstractions and higher-order variables. Like type theory, EFO has a type o of truth values and admits functions that take truth values to individuals. Such functions are not available in first-order logic. A typical example is a conditional $C : o \rightarrow o \rightarrow o$ taking a truth value and two individuals as arguments and returning one of the individuals. Here is a valid EFO formula that specifies the conditional and states one of its properties:

$$(\forall x y. C \perp x y = y \wedge C \top x y = x) \rightarrow C(x=y) x y = y$$

The starting point for EFO is an analytic tableau system derived from Brown's Henkin-complete cut-free one-sided sequent calculus for extensional type theory [2]. The tableau system is well-suited for proof search and yields decision procedures and the finite model property for three substantial fragments of EFO: lambda-free formulas (e.g., $pa \rightarrow pb \rightarrow p(a \wedge b)$), Bernays-Schönfinkel-Ramsey

formulas [4], and equations between pure lambda terms (terms not involving type o). The decidability and finite model results are mostly known, but it is remarkable that we obtain them with a single tableau system.

The proofs of the main results follow the usual development of first-order logic [9, 5], which applies the abstract consistency technique to a model existence lemma for the tableau system (Hintikka’s Lemma). Due to the presence of higher-order variables and lambda abstractions, the proof of the EFO model existence lemma is much harder than it is for first-order logic. We employ the possible-values technique [8], which has been used in [2] to obtain Henkin models, and in [3] to obtain standard models. We generalize the model existence theorem such that we can obtain countable models using the abstract consistency technique.

In a preceding paper [3], we develop a tableau-based decision procedure for the quantifier- and lambda-free fragment of EFO and introduce the possible-values-based construction of standard models. In this paper we extend the model construction to first-order quantification and lambda abstraction. We introduce a novel subterm restriction for the universal quantifier and employ an abstract normalization operator, both essential for proof search and decision procedures.

2 Basic Definitions

Types (σ, τ, μ) are obtained with the grammar $\tau ::= o \mid \iota \mid \tau\tau$. The elements of o are the two truth values, ι is interpreted as a nonempty set, and a function type $\sigma\tau$ is interpreted as the set of all total functions from σ to τ . For simplicity, we provide only one sort ι . Everything generalizes to countably many sorts.

We distinguish between two kinds of **names**, called **constants** and **variables**. Every name comes with a type. We assume that there are only countably many names, and that for every type there are infinitely many variables of this type. If not said otherwise, the letter a ranges over names, c over constants, and x and y over variables.

Terms (s, t, u, v) are obtained with the grammar $t ::= a \mid tt \mid \lambda x.t$ where an application st is only admitted if $s : \tau\mu$ and $t : \tau$ for some types τ and μ . Terms of type o are called **formulas**. A term is **lambda-free** if it does not contain a subterm that is a lambda abstraction. We use $\mathcal{N}s$ to denote the set of all names that have a free occurrence in the term s .

We assume that $\perp : o$, $\neg : oo$, $\wedge : ooo$, $=_\sigma : \sigma\sigma o$, and $\forall_\sigma : (\sigma o)o$ are constants for all types σ . We write $\forall x.s$ for $\forall_\sigma(\lambda x.s)$. An **interpretation** is a function \mathcal{I} that is defined on all types and all names and satisfies the following conditions:

- $\mathcal{I}o = \{0, 1\}$

- $\mathcal{I}(\sigma\tau)$ is the set of all total functions from $\mathcal{I}\sigma$ to $\mathcal{I}\tau$
- $\mathcal{I}\perp = 0$
- $\mathcal{I}(\neg)$, $\mathcal{I}(\wedge)$, $\mathcal{I}(=_\sigma)$, and $\mathcal{I}(\forall_\sigma)$ are the standard interpretations of the respective logical constants.

We write $\hat{\mathcal{I}}s$ for the value the term s evaluates to under the interpretation \mathcal{I} . We say that an interpretation \mathcal{I} is **countable** [**finite**] if $\mathcal{I}t$ is countable [finite]. An interpretation \mathcal{I} is a **model** of a set A of formulas if $\hat{\mathcal{I}}s = 1$ for every formula $s \in A$. A set of formulas is **satisfiable** if it has a model.

The constants \perp , \neg , \wedge , $=_t$, and \forall_t are called **EFO constants**. An **EFO term** is a term that contains no other constants but EFO constants. We write EFO_σ for the set of all EFO terms of type σ . For simplicity, we work with a restricted set of EFO constants. Everything generalizes to the remaining propositional constants, the identity $=_o$, and the existential quantifier \exists_t .

3 Normalization

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 $[s] = s$.

There are several possibilities for the normalization operator $[\]$: β -, long β -, or $\beta\eta$ -normal form, all possibly with standardized bound variables [7]. We will not commit to a particular operator but state explicitly the properties we require for our results. To start, we require the following properties:

$$\text{N1 } [[s]] = [s]$$

$$\text{N2 } [[s]t] = [st]$$

$$\text{N3 } [as_1 \dots s_n] = a[s_1] \dots [s_n] \text{ if the type of } as_1 \dots s_n \text{ is } o \text{ or } t$$

$$\text{N4 } \hat{\mathcal{I}}[s] = \hat{\mathcal{I}}s$$

Note that a ranges over names and \mathcal{I} ranges over interpretations. N3 also applies for $n = 0$.

Proposition 3.1 A term $as_1 \dots s_n$ of type o or t is normal iff s_1, \dots, s_n are normal.

Proof Follows from N3. ■

We need further properties of the normalization operator that can only be expressed with substitutions. A **substitution** is a type preserving partial function from variables to terms. If θ is a substitution, x is a variable, and s is a term that has the same type as x , we use θ_s^x to denote the substitution that agrees

$$\begin{array}{c}
\mathcal{T}_{\neg} \frac{s, \neg s}{\perp} \quad \mathcal{T}_{\neg\neg} \frac{\neg\neg s}{s} \quad \mathcal{T}_{\wedge} \frac{s \wedge t}{s, t} \quad \mathcal{T}_{\neg\wedge} \frac{\neg(s \wedge t)}{\neg s \mid \neg t} \\
\mathcal{T}_{\forall} \frac{\forall_t s}{[st]} \quad t : \iota \quad \mathcal{T}_{\neg\forall} \frac{\neg\forall_t s}{\neg[sx]} \quad x : \iota \text{ fresh} \\
\mathcal{T}_{\text{MAT}} \frac{\mathcal{X} s_1 \dots s_n, \neg \mathcal{X} t_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n} \quad \mathcal{T}_{\text{DEC}} \frac{\mathcal{X} s_1 \dots s_n \neq_t \mathcal{X} t_1 \dots t_n}{s_1 \neq t_1 \mid \dots \mid s_n \neq t_n} \\
\mathcal{T}_{\neq} \frac{s \neq s}{\perp} \quad \mathcal{T}_{\text{BE}} \frac{s \neq_o t}{s, \neg t \mid \neg s, t} \quad \mathcal{T}_{\text{FE}} \frac{s \neq_{\sigma\tau} t}{[sx] \neq [tx]} \quad x : \sigma \text{ fresh} \\
\mathcal{T}_{\text{CON}} \frac{s =_t t, u \neq_t v}{s \neq u, t \neq u \mid s \neq v, t \neq v}
\end{array}$$

Figure 1: Tableau system \mathcal{T}

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 $\hat{\theta}a = \text{if } a \in \text{Dom } \theta \text{ then } \theta a \text{ else } a$
- S2 $\hat{\theta}(st) = (\hat{\theta}s)(\hat{\theta}t)$
- S3 $[(\hat{\theta}(\lambda x.s))t] = [\hat{\theta}_t^x s]$
- S4 $[\hat{\theta}s] = [s]$
- S5 $\mathcal{N}[s] \subseteq \mathcal{N}s$ and $\mathcal{N}(\hat{\theta}s) \subseteq \bigcup \{ \mathcal{N}(\hat{\theta}a) \mid a \in \mathcal{N}s \}$

Note that a ranges over names and that \emptyset (the empty set) is the substitution that is undefined on every variable.

4 Tableau System

The results of this paper originate with the tableau system \mathcal{T} shown in Figure 1. The rules in the first two lines of Figure 1 are the familiar rules from first-order logic. The rules in the third and fourth line deal with embedded formulas. The **mating rule** \mathcal{T}_{MAT} decomposes complementary atomic formulas by introducing disequations that confront corresponding subterms. Disequations can be further decomposed with \mathcal{T}_{DEC} . Embedded formulas are eventually raised to the top level by Rule \mathcal{T}_{BE} , which incorporates Boolean extensionality. Rule \mathcal{T}_{FE} in-

incorporates functional extensionality. It reduces disequations at functional types to disequations at lower types. The confrontation rule \mathcal{T}_{CON} deals with positive equations at type ι . A discussion of the confrontation rule can be found in [3]. The tableau rules are such that they add normal formulas if they are applied to normal formulas.

Example 4.1 The following tableau refutes the formula $pf \wedge \neg p(\lambda x. \neg \neg fx)$ where $p : (\iota\omega)\omega$ and $f : \iota\omega$.

$$\begin{array}{c}
 pf \wedge \neg p(\lambda x. \neg \neg fx) \\
 pf, \neg p(\lambda x. \neg \neg fx) \\
 f \neq (\lambda x. \neg \neg fx) \\
 fx \neq \neg \neg fx \\
 \hline
 \begin{array}{c|c}
 fx, \neg \neg \neg fx & \neg fx, \neg \neg fx \\
 \neg fx & \perp \\
 \perp &
 \end{array}
 \end{array}$$

The rules used are \mathcal{T}_{\wedge} , \mathcal{T}_{MAT} , \mathcal{T}_{FE} , \mathcal{T}_{BE} , $\mathcal{T}_{\neg\neg}$, and \mathcal{T}_{\neg} . □

5 Evidence

A **quasi-EFO formula** is a disequation $s \neq_{\sigma} t$ such that s and t are EFO terms and $\sigma \neq \iota$. Note that the rules \mathcal{T}_{MAT} and \mathcal{T}_{DEC} may yield quasi-EFO formulas when they are applied to EFO formulas. A **branch** is a set of normal formulas s such that s is either EFO or quasi-EFO.

A term $s : \iota$ is **discriminating** in a branch A if A contains a disequation $s \neq t$ or $t \neq s$ for some term t . We use \mathcal{DA} to denote the set of all terms that are discriminating in a branch A .

Proposition 5.1 Let A be a branch. Then all terms in \mathcal{DA} are normal.

Proof Follows with N3 since a branch contains only normal formulas. ■

A branch E is **evident** if it satisfies the **evidence conditions** in Figure 2. The evidence conditions correspond to the tableau rules and are designed such that a branch that is closed under the tableau rules and does not contain \perp is evident. Note that the evidence conditions require less than the tableau rules:

1. \mathcal{E}_{\neg} is restricted to variables.
2. \mathcal{E}_{\forall} requires less instances than \mathcal{T}_{\forall} admits.
3. $\mathcal{E}_{\neg\forall}$ admits all EFO terms as witnesses.
4. \mathcal{E}_{\neq} is restricted to type ι .

\mathcal{E}_\perp	\perp is not in E .
\mathcal{E}_\neg	If $\neg x$ is in E , then x is not in E .
$\mathcal{E}_{\neg\neg}$	If $\neg\neg s$ is in E , then s is in E .
\mathcal{E}_\wedge	If $s \wedge t$ is in E , then s and t are in E .
$\mathcal{E}_{\neg\wedge}$	If $\neg(s \wedge t)$ is in E , then $\neg s$ or $\neg t$ is in E .
\mathcal{E}_\forall	If $\forall_i s$ is in E , then $[st]$ is in E for all $t \in \mathcal{DE}$, and $[st]$ is in E for some $t \in \text{EFO}_i$.
$\mathcal{E}_{\neg\forall}$	If $\neg\forall_i s$ is in E , then $\neg[st]$ is in E for some $t \in \text{EFO}_i$.
\mathcal{E}_{MAT}	If $x s_1 \dots s_n$ and $\neg x t_1 \dots t_n$ are in E where $n \geq 1$, then $s_i \neq t_i$ is in E for some $i \in \{1, \dots, n\}$.
\mathcal{E}_{DEC}	If $x s_1 \dots s_n \neq_i x t_1 \dots t_n$ is in E where $n \geq 1$, then $s_i \neq t_i$ is in E for some $i \in \{1, \dots, n\}$.
\mathcal{E}_\neq	If $s \neq_i t$ is in E , then s and t are different.
\mathcal{E}_{BE}	If $s \neq_o t$ is in E , then either s and $\neg t$ are in E or $\neg s$ and t are in E .
\mathcal{E}_{FE}	If $s \neq_{\sigma\tau} t$ is in E , then $[sx] \neq [tx]$ is in E for some variable x .
\mathcal{E}_{CON}	If $s =_i t$ and $u \neq_i v$ are in E , then either $s \neq u$ and $t \neq u$ are in E or $s \neq v$ and $t \neq v$ are in E .

Figure 2: Evidence conditions

In §7 we will show that every evident branch is satisfiable. In §9 we will prove the completeness of a tableau system \mathcal{R} that restricts the rule \mathcal{T}_\forall as suggested by the evidence condition \mathcal{E}_\forall .

Example 5.2 Let $p : (uu)o$. The following branch is evident.

$$p(\lambda xy.x), \neg p(\lambda xy.y), (\lambda xy.x) \neq (\lambda xy.y), (\lambda y.x) \neq (\lambda y.y), x \neq y \quad \square$$

Example 5.3 Let $f : io$ and $g : oi$ be variables. The branch

$$f(g(\forall_i f)), \neg f(g(\forall_i f)), g(\forall_i f) \neq_i g(\forall_i f), \forall_i f \neq_o \forall_i f, \forall_i f, \neg \forall_i f$$

is unsatisfiable and satisfies all evidence conditions but \mathcal{E}_\neq . Note that the mating rule does not apply to $\forall_i f$ and $\neg \forall_i f$ since \forall_i is a constant and not a variable. \square

6 Carriers

A carrier for an evident branch E consists of a set D and a relation $\triangleright_l \subseteq \text{EFO}_l \times D$ such that certain conditions are satisfied. We will show that every evident branch has carriers, and that for every carrier (D, \triangleright_l) for an evident branch E we can obtain a model \mathcal{I} of E such that $\mathcal{I}l = D$ and $s \triangleright_l \hat{\mathcal{I}}s$ for all $s \in \text{EFO}_l$. We call \triangleright_l a **possible-values relation** and read $s \triangleright_l a$ as **s can be a** . Given $s \triangleright_l a$, we say that a is a **possible value** for s .

We assume that some evident branch E is given. We say that a set $T \subseteq \text{EFO}_l$ is **compatible** if there are no terms $s, t \in T$ such that $([s] \neq [t]) \in E$. We write $s \# t$ if E contains the disequation $s \neq t$ or $t \neq s$.

Let a non-empty set D and a relation $\triangleright_l \subseteq \text{EFO}_l \times D$ be given. For $T \subseteq \text{EFO}_l$ and $a \in D$ we write $T \triangleright_l a$ if $t \triangleright_l a$ for every $t \in T$. For all terms $s, t \in \text{EFO}_l$, all values $a, b \in D$, and every set $T \subseteq \text{EFO}_l$ we require the following properties:

B1 $s \triangleright_l a$ iff $[s] \triangleright_l a$.

B2 T compatible iff $T \triangleright_l a$ for some $a \in D$.

B3 If $(s =_l t) \in E$ and $s \triangleright_l a$ and $t \triangleright_l b$, then $a = b$.

B4 For every $a \in D$ either $t \triangleright_l a$ for some $t \in \mathcal{DE}$ or $t \triangleright_l a$ for every $t \in \text{EFO}_l$.

Given an evident branch E , a **carrier for E** is a pair (D, \triangleright_l) as specified above.

6.1 Quotient-Based Carriers

A branch A is **complete** if for all $s, t \in \text{EFO}_l$ either $[s = t]$ is in A or $[s \neq t]$ is in A . We will show that complete evident branches have countable carriers that can be obtained as quotients of EFO_l with respect to the equations contained in the branch.

Let E be a complete evident branch in the following. We write $s \sim t$ if s and t are EFO terms of type l and $[s =_l t] \in E$. We define $\tilde{s} := \{ t \mid t \sim s \}$ for $s \in \text{EFO}_l$.

Proposition 6.1 For all $s, t \in \text{EFO}_l$: $s \sim t$ iff $[s \neq t] \in E$.

Proof One direction is obvious, the other follows with N3. ■

Proposition 6.2 \sim is an equivalence relation on EFO_l .

Proof We show symmetry by contradiction. Let $s \sim t$ and assume $t \not\sim s$. Then $[s = t]$ and $[t \neq s]$ are in E . By N3 we know that $[s] = [t]$ and $[t] \neq [s]$ are in E . By \mathcal{E}_{CON} either $[t] \neq [t]$ or $[s] \neq [s]$ is in E . Contradiction by \mathcal{E}_\neq . Reflexivity and transitivity follow with similar arguments. ■

Proposition 6.3 Let $T \subseteq \text{EFO}_l$. Then T is compatible iff $s \sim t$ for all $s, t \in T$.

Proof By definition and N3, T is compatible if $[s \neq t] \notin E$ for all $s, t \in T$. The claim follows with Proposition 6.1. ■

Lemma 6.4 Every complete evident branch has a countable carrier.

Proof Let E be a complete evident branch. We define:

$$D := \{ \tilde{s} \mid s \in \text{EFO}_l \}$$

$$s \triangleright_l \tilde{t} :\iff s \sim t$$

We will show that (D, \triangleright_l) is a carrier for E . Note that \triangleright_l is well-defined since \sim is an equivalence relation. D is countable since EFO_l is countable.

B1. We have to show that $s \sim t$ iff $[s] \sim t$. This follows with N3 and N1 since $s \sim t$ iff $[s=t] \in E$ and $[s] \sim t$ iff $[[s]=t] \in E$.

B2. If T is empty, B2 holds vacuously. Otherwise, let $t \in T$. Then T is compatible iff $s \sim t$ for all $s \in T$ by Propositions 6.3 and 6.2. Hence T is compatible iff $s \triangleright_l \tilde{t}$ for all $s \in T$. The claim follows.

B3. Let $s =_l t$ in E and $s \triangleright_l \tilde{u}$ and $t \triangleright_l \tilde{v}$. Since $s = t$ is normal, we have $s \sim t$. By definition of \triangleright_l we have $s \sim u$ and $t \sim v$. Hence $\tilde{u} = \tilde{v}$ since \sim is an equivalence relation.

B4. If \mathcal{DE} is empty, then $s \triangleright_l \tilde{t}$ for all $s, t \in \text{EFO}_l$ and hence the claim holds. Otherwise, let \mathcal{DE} be nonempty. We show the claim by contradiction. Suppose there is a term $t \in \text{EFO}_l$ such that $s \not\triangleright_l \tilde{t}$ for all $s \in \mathcal{DE}$. Then $[s \neq t] \in E$ for all $s \in \mathcal{DE}$ by Proposition 6.1. Since \mathcal{DE} is nonempty, we have $[t] \in \mathcal{DE}$ by N3. Thus $([t] \neq [t]) \in E$ by N3. Contradiction by $\mathcal{E}_\#$. ■

6.2 Discriminant-Based Carriers

We will now show that every evident branch has a carrier. Let an evident branch E be given. We will call a term **discriminating** if it is discriminating in E . A **discriminant** is a maximal set a of discriminating terms such that there is no disequation $s \neq t \in E$ such that $s, t \in a$. We will construct a carrier for E whose values are the discriminants.

Example 6.5 Suppose $E = \{x \neq y, x \neq z, y \neq z\}$ and $x, y, z : \iota$. Then there are 3 discriminants: $\{x\}, \{y\}, \{z\}$. □

Example 6.6 Suppose $E = \{x \neq f(fx), fx \neq f(f(fx))\}$ and $f : u$. Then there are 4 discriminants: $\{x, fx\}, \{x, f(f(fx))\}, \{f(fx), fx\}, \{f(fx), f(f(fx))\}$. □

Example 6.7 Suppose $E = \{a_n \neq_l b_n \mid n \in \mathbb{N}\}$ where the a_n and b_n are pairwise distinct constants. Then E is evident and there are uncountably many discriminants. \square

Proposition 6.8 If E contains exactly n disequations at ι , then there are at most 2^n discriminants. If E contains no disequation at ι , then \emptyset is the only discriminant.

Proposition 6.9 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 $s \# t$.
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 $s \# t$. Let $s \in a$. Then $s \in b$ since b is a maximal compatible 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 $s \# t$. By \mathcal{E}_{CON} we have $s_1 \# s$ or $s_2 \# t$. Contradiction since a and b are discriminants. \blacksquare

Lemma 6.10 Every (finite) evident branch has a (finite) carrier.

Proof Let E be an evident branch. We define:

$$D := \text{set of all discriminants}$$

$$s \triangleright_\iota a := \Leftrightarrow ([s] \text{ discriminating} \Rightarrow [s] \in a)$$

We will show that $(D, \triangleright_\iota)$ is a carrier for E . By Proposition 6.8 we know that D is finite if E is finite.

B1. Holds by N1.

For the remaining carrier conditions we distinguish two cases. If $\mathcal{D}E = \emptyset$, then \emptyset is the only discriminant and B2, B3, and B4 are easily verified. Otherwise, let $\mathcal{D}E \neq \emptyset$.

B2 \Rightarrow . Let T be compatible. Then there exists a discriminant a that contains all the discriminating terms in $\{[t] \mid t \in T\}$. The claim follows since $T \triangleright a$.

B2 \Leftarrow . By contradiction. 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.

B3. Let $(s=t) \in E$ and $s \triangleright_\iota a$ and $t \triangleright_\iota b$. We show $a = b$. Since there are discriminating terms, E contains at least one disequation at type ι , and hence s and t are discriminating by \mathcal{E}_{CON} . By N3 s and t are normal and hence $s \in a$ and $t \in b$. Now $a = b$ by Proposition 6.9(2).

B4. Since there are discriminating terms, we know by \mathcal{E}_\neq that every discriminant contains at least one discriminating term. Since discriminating terms are normal, we have the claim. ■

7 Model Existence

We will now show that every evident branch has a model.

Lemma 7.1 (Model Existence) Let $(D, \triangleright_\iota)$ be a carrier for an evident branch E . Then E has a model \mathcal{I} such that $\mathcal{I}\iota = D$.

We start the proof of Lemma 7.1. Let $(D, \triangleright_\iota)$ be a carrier for an evident branch E . For the rest of the proof we only consider interpretations \mathcal{I} such that $\mathcal{I}\iota = D$.

7.1 Possible Values

To obtain a model of E , we need suitable values for all variables. We address this problem by defining possible-values relations $\triangleright_\sigma \subseteq \text{EFO}_\sigma \times \mathcal{I}\sigma$ for all types $\sigma \neq \iota$:

$$\begin{aligned} s \triangleright_o 0 &: \iff [s] \notin E \\ s \triangleright_o 1 &: \iff \neg[s] \notin E \\ s \triangleright_{\sigma\tau} f &: \iff st \triangleright_\tau fa \text{ whenever } t \triangleright_\sigma a \end{aligned}$$

Note that we already have a possible-values relation for ι and that the definition of the possible values relations for functional types is by induction on types. Also note that if s is an EFO formula such that $[s] \notin E$ and $\neg[s] \notin E$, then both 0 and 1 are possible values for s . We will show that every EFO term has a possible value and that we obtain a model of E if we define $\mathcal{I}x$ as a possible value for x for every variable x .

Proposition 7.2 Let $s \in \text{EFO}_\sigma$ and $a \in \mathcal{I}\sigma$. Then $s \triangleright_\sigma a \iff [s] \triangleright_\sigma a$.

Proof By induction on σ . For o the claim follows with N1. For ι the claim follows with B1. Let $\sigma = \tau\mu$.

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

Suppose $[s] \triangleright_\sigma a$. Let $t \triangleright_\tau b$. Then $[s]t \triangleright_\mu ab$. By inductive hypothesis $[[s]t] \triangleright_\mu ab$. Thus $[st] \triangleright_\mu ab$ by N2. By inductive hypothesis $st \triangleright_\mu ab$. Hence $s \triangleright_\sigma a$. ■

Lemma 7.3 For every EFO constant c : $c \triangleright \mathcal{I}c$.

Proof

$c = \perp$. The claim follows by \mathcal{E}_\perp and N3.

$c = \neg$. Assume $s \triangleright_o a$. We show $\neg s \triangleright \mathcal{I}(\neg)a$ by contradiction. Suppose $\neg s \not\triangleright \mathcal{I}(\neg)a$. Case analysis.

$a = 0$. Then $[s] \notin E$ and $\neg[\neg s] \in E$. Thus $\neg\neg[s] \in E$ by N3. Hence $[s] \in E$ by $\mathcal{E}_{\neg\neg}$. Contradiction.

$a = 1$. Then $\neg[s] \notin E$ and $[\neg s] \in E$. Contradiction by N3.

$c = \wedge$. Assume $s \triangleright_o a$ and $t \triangleright_o b$. We show $s \wedge t \triangleright \mathcal{I}(\wedge)ab$ by contradiction. Suppose $s \wedge t \not\triangleright \mathcal{I}(\wedge)ab$. Case analysis.

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

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

$c = (=)$. Assume $s \triangleright_i a$ and $t \triangleright_i b$. We show $(s=t) \triangleright \mathcal{I}(=)ab$ by contradiction. Suppose $(s=t) \not\triangleright \mathcal{I}(=)ab$. Case analysis.

$a = b$. Then $\neg[s=t] \in E$ and $s, t \triangleright_i a$. By B2 $\{s, t\}$ is compatible. Contradiction by N3.

$a \neq b$. Then $([s]=[t]) \in E$ by N3. Hence $a = b$ by B1 and B3. Contradiction.

$c = \forall_i$. Assume $s \triangleright_{io} f$. We show $\forall_i s \triangleright_o \mathcal{I}\forall_i f$ by contradiction. Suppose $\forall_i s \not\triangleright_o \mathcal{I}\forall_i f$. Case analysis.

$\mathcal{I}\forall_i f = 0$. Then $\forall_i [s] \in E$ by N3 and $fa = 0$ for some value a . By \mathcal{E}_\forall and B4 there exists a term t such that $[[s]t] \in E$ and $t \triangleright_i a$. Thus $st \triangleright fa = 0$ and hence $[st] \notin E$. Contradiction by N2.

$\mathcal{I}\forall_i f = 1$. Then $\neg\forall_i [s] \in E$ by N3. By $\mathcal{E}_{\neg\forall}$ we have $\neg[[s]t] \in E$ for some term $t \in \text{EFO}_i$. By \mathcal{E}_\neq and B2 we have $t \triangleright a$ for some value a . Now $st \triangleright fa = 1$. Thus $\neg[st] \notin E$. Contradiction by N2. ■

We call an interpretation \mathcal{I} **admissible** if it satisfies $x \triangleright \mathcal{I}x$ for every variable x . We will show that admissible interpretations exist and that every admissible interpretation is a model of E .

Lemma 7.4 (Admissibility) Let \mathcal{I} be admissible and θ be a substitution such that $\theta x \triangleright \mathcal{I}x$ for all $x \in \text{Dom } \theta$. Then $\hat{\theta}s \triangleright \hat{\mathcal{I}}s$ for every EFO term s .

Proof By induction on s . Let s be an EFO term. By assumption, θx is EFO for all $x \in \text{Dom } \theta$. Hence $\hat{\theta}s$ is EFO by S5. Case analysis.

$s = a$. If $a \in \text{Dom } \theta$, the claim holds by assumption. If $a \notin \text{Dom } \theta$, then $\hat{\theta}s = a$ by S1. If a is a constant, the claim holds by Lemma 7.3. If a is a variable, the claim holds by assumption.

$s = tu$. Then $\hat{\theta}s = (\hat{\theta}t)(\hat{\theta}u)$ by S2. Now $\hat{\theta}t \triangleright \hat{\mathcal{I}}t$ and $\hat{\theta}u \triangleright \hat{\mathcal{I}}u$ by the inductive hypothesis. Now $\hat{\theta}s = (\hat{\theta}t)(\hat{\theta}u) \triangleright (\hat{\mathcal{I}}t)(\hat{\mathcal{I}}u) = \hat{\mathcal{I}}s$.

$s = \lambda x.t$ and $x : \sigma$. Moreover, let $u \triangleright_\sigma a$. We show $(\hat{\theta}s)u \triangleright (\hat{\mathcal{I}}s)a$. By Proposition 7.2 it suffices to show $[(\hat{\theta}s)u] \triangleright (\hat{\mathcal{I}}s)a$. We have $[(\hat{\theta}s)u] = [\hat{\theta}_u^x t]$ by S3 and $(\hat{\mathcal{I}}s)a = \hat{\mathcal{I}}_a^x t$ where $\hat{\mathcal{I}}_a^x$ denotes the interpretation that agrees everywhere with \mathcal{I} but possibly on x where it yields a . By inductive hypothesis we have $\hat{\theta}_u^x t \triangleright \hat{\mathcal{I}}_a^x t$. The claim follows with Proposition 7.2. \blacksquare

7.2 Compatibility

It remains to show that there is an admissible interpretation and that every admissible interpretation is a model of E . For this purpose we define compatibility relations $\parallel_\sigma \subseteq \text{EFO}_\sigma \times \text{EFO}_\sigma$ for all types:

$$\begin{aligned} s \parallel_o t &: \iff \{[s], \neg[t]\} \notin E \text{ and } \{\neg[s], [t]\} \notin E \\ s \parallel_l t &: \iff \text{not } [s] \# [t] \\ s \parallel_{\sigma\tau} t &: \iff su \parallel_\tau tv \text{ whenever } u \parallel_\sigma v \end{aligned}$$

Note that the definition of the compatibility relations for functional types is by induction on types. We say that s and t are **compatible** if $s \parallel t$. A set T of equi-typed terms is **compatible** if $s \parallel t$ for all terms $s, t \in T$. If $T \subseteq \text{EFO}_\sigma$, we write $T \triangleright a$ if a is a common possible value for all terms $s \in T$. We will show that a set of equi-typed terms is compatible if and only if all its terms have a common possible value.

Proposition 7.5 The compatibility relations \parallel_σ are symmetric.

The compatibility relations are also reflexive. Showing this fact will take some effort. We first show $x \parallel x$ for all variables x . For the induction to go through we strengthen the hypothesis.

Lemma 7.6 (Reflexivity) For every type σ and all EFO terms $s, t, xs_1 \dots s_n, xt_1 \dots t_n$ of type σ with $n \geq 0$:

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

Proof By mutual induction on σ . The base cases for Claim (1) follow by contradiction. For $\sigma = o$ \mathcal{E}_{BE} is needed. The base cases for Claim (2) follow with N3, \mathcal{E}_{MAT} , \mathcal{E}_{DEC} , \mathcal{E}_{\neg} , and \mathcal{E}_{\neq} . We now show the claims for $\sigma = \tau\mu$.

1. By contradiction. Suppose $s \parallel_{\sigma} t$ and $[s] \# [t]$. By \mathcal{E}_{FE} $[[s]x] \# [[t]x]$ 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.
2. Suppose $x s_1 \dots s_n \not\parallel_{\sigma} x t_1 \dots t_n$. Then there exist terms such that $u \parallel_{\tau} v$ and $x s_1 \dots s_n u \not\parallel_{\mu} x t_1 \dots t_n v$. By inductive hypothesis (1) we know that $[u] \# [v]$ does not hold. Hence $[s_i] \# [t_i]$ for some $i \in \{1, \dots, n\}$ by inductive hypotheses (2). ■

Lemma 7.7 (Common Value) Let $T \subseteq \text{EFO}_{\sigma}$. Then T is compatible if and only if there exists a value a such that $T \triangleright_{\sigma} a$.

Proof By induction on σ . For $\sigma = \iota$ the claim is identical with B2.

$\sigma = o$, \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 $s \not\parallel t$. Hence T is not compatible.

$\sigma = o$, \Leftarrow . By contraposition. Suppose $s \not\parallel_o t$ 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 $T_a \triangleright_{\mu} f a$ 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 $su, tv \triangleright_{\mu} f a$. Thus $su \parallel_{\mu} tv$ by the inductive hypothesis. ■

Lemma 7.8 Every admissible interpretation is a model of E .

Proof Let \mathcal{I} be an admissible interpretation and $s \in E$. We show $\hat{\mathcal{I}}s = 1$. Case analysis.

Suppose s is a normal EFO term. Then $s = [s] = [\hat{\theta}s]$ by S4 and $s \not\triangleright 0$. Moreover, $\hat{\theta}s \triangleright \hat{\mathcal{I}}s$ by Lemma 7.4 and $s \triangleright \hat{\mathcal{I}}s$ by Lemma 7.2. Hence $\hat{\mathcal{I}}s = 1$.

Suppose $s = (t \neq u)$ where t and u are normal EFO terms. Then $t = [t] = [\hat{\theta}t]$ and $u = [u] = [\hat{\theta}u]$ by S4. We prove the claim by contradiction. Suppose $\hat{\mathcal{I}}s = 0$. Then $\hat{\mathcal{I}}t = \hat{\mathcal{I}}u$. Thus $\hat{\theta}t, \hat{\theta}u \triangleright \hat{\mathcal{I}}t$ by Lemma 7.4 and $t, u \triangleright \hat{\mathcal{I}}t$ by Lemma 7.2. Hence

$t \parallel u$ by Lemma 7.7. Thus not $[t] \# [u]$ by Lemma 7.6(1). Contradiction since $([t] \# [u]) \in E$. ■

We can now prove Lemma 7.1. By Lemma 7.6(2) we know $x \parallel x$ for every variable x . Hence there exists an admissible interpretation \mathcal{I} by Lemma 7.7. By Lemma 7.8 we know that \mathcal{I} is a model of E . This finishes the proof of Lemma 7.1.

Theorem 7.9 (Finite Model Existence)

Every finite evident branch has a finite model.

Proof Follows with Lemmas 6.10 and 7.1. ■

Lemma 7.10 (Model Existence) Let E be an evident branch. Then E has a model. Moreover, E has a countable model if E is complete.

Proof Follows with Lemmas 6.10, 7.1, and 6.4. ■

8 Abstract Consistency

To obtain our main results, we boost the model existence lemma with the abstract consistency technique. Everything works out smoothly.

An **abstract consistency class** is a set Γ of branches such that every branch $A \in \Gamma$ satisfies the conditions in Figure 3. An abstract consistency class Γ is **complete** if for every $A \in \Gamma$ and all $s, t \in \text{EFO}_l$ either $A \cup \{[s=t]\}$ is in Γ or $A \cup \{[s \neq t]\}$ is in Γ .

Proposition 8.1 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 8.2 (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, \dots be an enumeration of all formulas that can occur on a branch. We construct a sequence $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$ 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 four subcases.

1. If u_n is of the form $\forall_l s$, then choose A_{n+1} to be $B \cup \{[st]\} \in \Gamma$ for some $t \in \text{EFO}_l$. This is possible since Γ satisfies C_{\forall} .

- C_{\perp} \perp is not in A .
- C_{\neg} If $\neg x$ is in A , then x is not in A .
- $C_{\neg\neg}$ If $\neg\neg s$ is in A , then $A \cup \{s\}$ is in Γ .
- C_{\wedge} If $s \wedge t$ is in A , then $A \cup \{s, t\}$ is in Γ .
- $C_{\neg\wedge}$ If $\neg(s \wedge t)$ is in A , then $A \cup \{\neg s\}$ or $A \cup \{\neg t\}$ is in Γ .
- C_{\forall} If $\forall_t s$ is in A , then $A \cup \{[st]\}$ is in Γ for all $t \in \mathcal{D}A$,
and $A \cup \{[st]\}$ is in Γ for some $t \in \text{EFO}_t$.
- $C_{\neg\forall}$ If $\neg\forall_t s$ is in A , then $A \cup \{\neg[st]\}$ is in Γ for some $t \in \text{EFO}_t$.
- C_{MAT} If $x s_1 \dots s_n$ is in A and $\neg x t_1 \dots t_n$ 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_{DEC} If $x s_1 \dots s_n \neq_t x t_1 \dots t_n$ 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 $s \neq_t t$ is in A , then s and t are different.
- C_{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_{FE} If $s \neq_{\sigma\tau} t$ is in A , then $A \cup \{[sx] \neq [tx]\}$ is in Γ for some variable x .
- C_{CON} If $s =_t t$ and $u \neq_t v$ 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 .

Figure 3: Abstract consistency conditions (must hold for every $A \in \Gamma$)

2. If u_n is of the form $\neg\forall_t s$, then choose A_{n+1} to be $B \cup \{\neg[st]\} \in \Gamma$ for some $t \in \text{EFO}_t$. This is possible since Γ satisfies $C_{\neg\forall}$.
3. 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} .
4. If u_n has none of these forms, then let A_{n+1} be B .

Let $E := \bigcup_{n \in \mathbb{N}} A_n$. Note that $\mathcal{D}E = \bigcup_{n \in \mathbb{N}} \mathcal{D}A_n$. We show that E is evident.

- \mathcal{E}_{\perp} If \perp is in E , then \perp is in A_n for some n , contradicting C_{\perp} .
- \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}_{\neq} If $s \neq_t s$ is in E , then $s \neq_t s$ is in A_n for some n , contradicting C_{\neq} .
- $\mathcal{E}_{\neg\neg}$ Assume $\neg\neg s$ is in E . Let n be such that $u_n = s$ and $r \geq n$ be such that $\neg\neg s$ is in A_r . Since $A_n \cup \{s\} \subseteq A_r \cup \{s\} \in \Gamma$ (using $C_{\neg\neg}$), we have $s \in A_{n+1} \subseteq E$.
- \mathcal{E}_{\wedge} Assume $s \wedge t$ is in E . Let n, m be such that $u_n = s$ and $u_m = t$. Let $r \geq n, m$ be such that $s \wedge t$ is in A_r . By C_{\wedge} , $A_r \cup \{s, t\} \in \Gamma$. Since $A_n \cup \{s\} \subseteq A_r \cup \{s, t\}$,

we have $s \in A_{n+1} \subseteq E$. Since $A_m \cup \{t\} \subseteq A_r \cup \{s, t\}$, we have $t \in A_{m+1} \subseteq E$.

$\mathcal{E}_{\neg\wedge}$ Assume $\neg(s \wedge t)$ is in E . Let n, m be such that $u_n = s$ and $u_m = t$. Let $r \geq n, m$ be such that $\neg(s \wedge t)$ is in A_r . By $C_{\neg\wedge}$, $A_r \cup \{\neg s\} \in \Gamma$ or $A_r \cup \{\neg t\} \in \Gamma$. 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, $A_m \cup \{\neg t\} \subseteq A_r \cup \{\neg t\} \in \Gamma$, and so $\neg t \in A_{m+1} \subseteq E$. Hence either $\neg s$ or $\neg t$ is in E .

\mathcal{E}_{\forall} Assume $\forall_t s$ is in E . Case analysis.

$DE = \emptyset$. Let n be such that $u_n = \forall_t s$. Let $r \geq n$ be such that $\forall_t s$ is in A_r .

By C_{\forall} there is some t such that $A_r \cup \{[st]\}$ is in Γ . Hence $[st] \in A_{n+1} \subseteq E$ for some t .

$DE \neq \emptyset$. Let $t \in DE$. We show $[st] \in E$. Let n be such that $u_n = [st]$. Let $r \geq n$ be such that $\forall_t s$ is in A_r and $t \in DA_r$. By C_{\forall} we have $A_r \cup \{[st]\} \in \Gamma$.

Since $A_n \cup \{u_n\} \subseteq A_r \cup \{[st]\}$, we have $[st] = u_n \in A_{n+1} \subseteq E$.

$\mathcal{E}_{\neg\forall}$ Assume $\neg\forall_t s$ is in E . Let n be such that $u_n = \neg\forall_t s$. Let $r \geq n$ be such that $\neg\forall_t s$ is in A_r . By $C_{\neg\forall}$ we know $A_r \cup \{\neg[st]\} \in \Gamma$ for some t . Hence $\neg[st] \in A_{n+1} \subseteq E$ for some t .

\mathcal{E}_{MAT} Assume $x s_1 \dots s_n$ and $\neg x t_1 \dots t_n$ are in E for some $n \geq 1$. For each $i \in \{1, \dots, n\}$, let m_i be such that u_{m_i} is $s_i \neq t_i$. Let $r \geq m_1, \dots, m_n$ be such that $x s_1 \dots s_n$ and $\neg x t_1 \dots t_n$ are in A_r . By C_{MAT} there is some $i \in \{1, \dots, n\}$ such that $A_r \cup \{s_i \neq t_i\} \in \Gamma$. Since $A_n \cup \{s_i \neq t_i\} \subseteq A_r \cup \{s_i \neq t_i\}$, we have $(s_i \neq t_i) \in A_{n+1} \subseteq E$.

\mathcal{E}_{DEC} Assume $x s_1 \dots s_n \neq_t x t_1 \dots t_n$ is in E for some $n \geq 1$. For each $i \in \{1, \dots, n\}$, let m_i be such that u_{m_i} is $s_i \neq t_i$. Let $r \geq m_1, \dots, m_n$ be such that $x s_1 \dots s_n \neq_t x t_1 \dots t_n$ is in A_r . By C_{DEC} there is some $i \in \{1, \dots, n\}$ such that $A_r \cup \{s_i \neq t_i\} \in \Gamma$. Since $A_n \cup \{s_i \neq t_i\} \subseteq A_r \cup \{s_i \neq t_i\}$, we have $(s_i \neq t_i) \in A_{n+1} \subseteq E$.

\mathcal{E}_{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 C_{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}_{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 $A_{n+1} \subseteq E$.

\mathcal{E}_{CON} Assume $s =_l t$ and $u \neq_l v$ 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 $s =_l t$ and $u \neq_l v$ 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 $t \neq v \in A_{k+1} \subseteq E$.

It remains to show that E is complete if Γ is complete. Let Γ be complete and $s, t \in \text{EFO}_i$. We show that $[s = t]$ or $[s \neq t]$ is in E . Let m, n be such that $u_m = [s=t]$ and $u_n = [s \neq t]$. We consider $m < n$, the case $m > n$ is symmetric. If $[s=t] \in A_n$, we have $[s=t] \in E$. If $[s=t] \notin A_n$, then $A_n \cup \{[s=t]\}$ is not in Γ . Hence $A_n \cup \{[s \neq t]\}$ is in Γ since Γ is complete. Hence $[s \neq t] \in A_{n+1} \subseteq E$. ■

9 Completeness

We will now show that the tableau system \mathcal{T} is complete. In fact, we will show the completeness of a tableau system \mathcal{R} that is obtained from \mathcal{T} by restricting the applicability of some of the rules. We consider \mathcal{R} since it provides for more focused proof search and also yields a decision procedure for three substantial fragments of EFO. \mathcal{R} is obtained from \mathcal{T} by restricting the applicability of the rules \mathcal{T}_\forall , $\mathcal{T}_{\neg\forall}$, and \mathcal{T}_{FE} as follows:

- \mathcal{T}_\forall can only be applied to $\forall_i s \in A$ with a term $t \in \text{EFO}_i$ if either $t \in \mathcal{DA}$ or the following conditions are satisfied:
 1. $\mathcal{DA} = \emptyset$ and t is a variable.
 2. $t \in \mathcal{NA}$ or $\mathcal{NA} = \emptyset$.
 3. There is no $u \in \text{EFO}_i$ such that $[su] \in A$.
- $\mathcal{T}_{\neg\forall}$ can only be applied to $\neg\forall_i s \in A$ if there is no $t \in \text{EFO}_i$ such that $\neg[st] \in A$.
- \mathcal{T}_{FE} can only be applied to an equation $(s =_{\sigma\tau} t) \in A$ if there is no variable $x : \sigma$ such that $([sx] = [tx]) \in A$.

We use \mathcal{R}_\forall , $\mathcal{R}_{\neg\forall}$, and \mathcal{R}_{FE} to refer to the restrictions of \mathcal{T}_\forall , $\mathcal{T}_{\neg\forall}$, and \mathcal{T}_{FE} , respectively. Note that \mathcal{R}_\forall provides a novel subterm restriction that may be useful for proof search. We say a branch A is **refutable** if it can be refuted with \mathcal{R} . Let $\Gamma_{\mathcal{T}}$ be the set of all finite branches that are not refutable.

Lemma 9.1 $\Gamma_{\mathcal{T}}$ is an abstract consistency class.

Proof We have to show that $\Gamma_{\mathcal{T}}$ satisfies the abstract consistency conditions. We prove some of the conditions, the verification of the remaining conditions is straightforward.

- C_{\perp} Suppose $\perp \in A \in \Gamma_{\mathcal{T}}$. Then A is refutable. Contradiction.
- C_{\neg} Suppose $\neg x, x \in A \in \Gamma_{\mathcal{T}}$. Then we can refute A using \mathcal{T}_{\neg} . Contradiction.
- $C_{\neg \wedge}$ Let $\neg(s \wedge t) \in A \in \Gamma_{\mathcal{T}}$. Suppose $A \cup \{\neg s\}$ and $A \cup \{\neg t\}$ are not in $\Gamma_{\mathcal{T}}$. Then $A \cup \{\neg s\}$ and $A \cup \{\neg t\}$ are refutable. Hence A can be refuted using $\mathcal{T}_{\neg \wedge}$. Contradiction.
- C_{\forall} Let $\forall t s \in A \in \Gamma_{\mathcal{T}}$. Suppose $A \cup \{[st]\} \notin \Gamma_{\mathcal{T}}$ for some $t \in \mathcal{DA}$ or $A \cup \{[st]\} \notin \Gamma_{\mathcal{T}}$ for all $t \in \text{EFO}_t$. Then $A \cup \{[st]\}$ is refutable for some $t \in \mathcal{DA}$ or $A \cup \{[st]\}$ is refutable for all $t \in \text{EFO}_t$. Hence A can be refuted using \mathcal{T}_{\forall} .
- $C_{\neg \forall}$ Let $\neg \forall t s \in A \in \Gamma_{\mathcal{T}}$. Suppose $A \cup \{\neg[st]\} \notin \Gamma_{\mathcal{T}}$ for every $t \in \text{EFO}_t$. Then $A \cup \{\neg[st]\}$ is refutable for every $t \in \text{EFO}_t$. Hence A is refutable using $\mathcal{T}_{\neg \forall}$ and the finiteness of A . Contradiction.
- C_{FE} Let $(s \neq_{\sigma} t) \in A \in \Gamma_{\mathcal{T}}$. 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}_{FE} and the finiteness of A . Contradiction. ■

Theorem 9.2 (Completeness)

\mathcal{T} and \mathcal{R} can refute every unsatisfiable finite branch.

Proof It suffice to show the claim for \mathcal{R} . We prove the claim 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 Lemmas 9.1, 8.2, and 7.10. ■

10 Compactness and Countable Models

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 $\Gamma_{\mathcal{C}}$ be the set of all sufficiently pure branches A such that every finite subset of A is satisfiable. We write \sqsubseteq_f for the finite subset relation.

Lemma 10.1 Let $A \in \Gamma_{\mathcal{C}}$ and B_1, \dots, B_n be finite branches such that $A \cup B_i \notin \Gamma_{\mathcal{C}}$ for all $i \in \{1, \dots, n\}$. Then there exists a finite branch $A' \sqsubseteq_f A$ such that $A' \cup B_i$ is unsatisfiable for all $i \in \{1, \dots, n\}$.

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

Lemma 10.2 $\Gamma_{\mathcal{C}}$ is a complete abstract consistency class.

Proof We verify the abstract consistency conditions as follows. Lemma 10.1 is used tacitly.

- C_{\perp} We cannot have $\perp \in A$ since $\{\perp\}$ would be an unsatisfiable finite subset.
- C_{\neg} We cannot have $\{\neg x, x\} \subseteq A$ since this would be an unsatisfiable finite subset.
- C_{\neq} We cannot have $(s \neq_l s) \in A$ since $\{s \neq s\}$ would be an unsatisfiable finite subset.
- $C_{\neg\neg}$ Assume $\neg\neg s \in A$ and $A \cup \{s\} \notin \Gamma_C$. There is a finite subset $A' \subseteq_f A$ such that $A' \cup \{s\}$ is unsatisfiable. There is a model of $A' \cup \{\neg\neg s\} \subseteq_f A$. This is also a model of $A' \cup \{s\}$, contradicting our choice of A' .
- C_{\wedge} Assume $s \wedge t$ is in A and $A \cup \{s, t\} \notin \Gamma_C$. There is some $A' \subseteq_f A$ such that $A' \cup \{s, t\}$ is unsatisfiable. There is a model of $A' \cup \{s \wedge t\} \subseteq_f A$. This is also a model of $A' \cup \{s, t\}$, contradicting our choice of A' .
- $C_{\neg\wedge}$ Assume $\neg(s \wedge t)$ is in A , $A \cup \{\neg s\} \notin \Gamma_C$ and $A \cup \{\neg t\} \notin \Gamma_C$. There is some $A' \subseteq_f A$ such that $A' \cup \{\neg s\}$ and $A' \cup \{\neg t\}$ are unsatisfiable. There is a model of $A' \cup \{\neg(s \wedge t)\} \subseteq_f A$. This is also a model of either $A' \cup \{\neg s\}$ or $A' \cup \{\neg t\}$, contradicting our choice of A' .
- C_{MAT} Assume $xs_1 \dots s_n$ and $\neg xt_1 \dots t_n$ are in A and $A \cup \{s_i \neq t_i\} \notin \Gamma_C$ for all $i \in \{1, \dots, n\}$. There is some $A' \subseteq_f A$ such that $A' \cup \{s_i \neq t_i\}$ is unsatisfiable for all $i \in \{1, \dots, n\}$. There is a model \mathcal{I} of $A' \cup \{xs_1 \dots s_n, \neg xt_1 \dots t_n\} \subseteq_f A$. Since $\hat{\mathcal{I}}(xs_1 \dots s_n) \neq \hat{\mathcal{I}}(\neg xt_1 \dots t_n)$, we must have $\hat{\mathcal{I}}(s_i) \neq \hat{\mathcal{I}}(t_i)$ for some $i \in \{1, \dots, n\}$. Thus \mathcal{I} models $A' \cup \{s_i \neq t_i\}$, contradicting our choice of A' .
- C_{DEC} Assume $xs_1 \dots s_n \neq_l xt_1 \dots t_n$ is in A and $A \cup \{s_i \neq t_i\} \notin \Gamma_C$ for all $i \in \{1, \dots, n\}$. There is some $A' \subseteq_f A$ such that $A' \cup \{s_i \neq t_i\}$ is unsatisfiable for all $i \in \{1, \dots, n\}$. There is a model \mathcal{I} of $A' \cup \{xs_1 \dots s_n \neq_l xt_1 \dots t_n\} \subseteq_f A$. Since $\hat{\mathcal{I}}(xs_1 \dots s_n) \neq \hat{\mathcal{I}}(\neg xt_1 \dots t_n)$, we must have $\hat{\mathcal{I}}(s_i) \neq \hat{\mathcal{I}}(t_i)$ for some $i \in \{1, \dots, n\}$. Thus \mathcal{I} models $A' \cup \{s_i \neq t_i\}$, contradicting our choice of A' .
- C_{BE} Assume $s \neq_o t$ is in A , $A \cup \{s, \neg t\} \notin \Gamma_C$ and $A \cup \{\neg s, t\} \notin \Gamma_C$. 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 $A' \cup \{\neg s, t\}$.
- C_{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 $A \cup \{[sx] \neq [tx]\} \notin \Gamma_C$. 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 $\hat{\mathcal{I}}_a^x(sx) \neq \hat{\mathcal{I}}_a^x(tx)$ and \mathcal{I}_a^x is a model of A' . Since $\hat{\mathcal{I}}_a^x([sx]) = \hat{\mathcal{I}}_a^x(sx)$ by N4 and $\hat{\mathcal{I}}_a^x([tx]) = \hat{\mathcal{I}}_a^x(tx)$, we conclude \mathcal{I}_a^x is a model of $A' \cup \{[sx] \neq [tx]\}$, contradicting our choice of A' .
- C_{CON} Assume $s =_l t$ and $u \neq_l v$ 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' .

C_{\forall} Assume $\forall_t s$ is in A and $A \cup \{[st]\} \notin \Gamma_C$ for some $t \in \text{EFO}_t$. There is some $A' \subseteq_f A$ such that $A' \cup \{[st]\}$ is unsatisfiable. There is a model \mathcal{I} of $A' \cup \{\forall_t s\} \subseteq_f A$. Note that $\hat{\mathcal{I}}([st]) = \hat{\mathcal{I}}(st) = \hat{\mathcal{I}}(s)(\hat{\mathcal{I}}(t)) = 1$ using N4. Hence \mathcal{I} is a model of $A' \cup \{[st]\}$, contradicting our choice of A' .

$C_{\neg\forall}$ Assume $\neg\forall_t s$ is in A . Since A is sufficiently pure, there is a variable x_t which does not occur in A . Assume $A \cup \{\neg[sx]\} \notin \Gamma_C$. There is some $A' \subseteq_f A$ such that $A' \cup \{\neg[sx]\}$ is unsatisfiable. There is a model \mathcal{I} of $A' \cup \{\neg\forall_t s\} \subseteq_f A$. There is some $a \in \mathcal{I}_t$ such that $\hat{\mathcal{I}}(s)a = 0$. Since x does not occur in A , we know $\hat{\mathcal{I}}_a^x(s)a = \hat{\mathcal{I}}(s)a = 0$ and \mathcal{I}_a^x is a model of A' . Note that $\hat{\mathcal{I}}_a^x([sx]) = \hat{\mathcal{I}}_a^x(sx) = \hat{\mathcal{I}}_a^x(s)a = 0$ using N4. Hence \mathcal{I} is a model of $A' \cup \{\neg[sx]\}$, contradicting our choice of A' .

We show the completeness of Γ_C by contradiction. Let $A \in \Gamma_C$ and $s, t \in \text{EFO}_t$ such that $A \cup \{[s=t]\}$ and $A \cup \{[s \neq t]\}$ are not in Γ_C . Then there exists $A' \subseteq_f A$ such that $A' \cup \{[s=t]\}$ and $A' \cup \{[s \neq t]\}$ are unsatisfiable. Contradiction by N4 since A' is satisfiable. ■

Theorem 10.3 (Compactness)

A branch is satisfiable if each of its finite subsets is satisfiable.

Proof Let A be a branch such that every finite subset of A is satisfiable. Without loss of generality we assume A is sufficiently pure. Then $A \in \Gamma_C$. Hence A is satisfiable by Lemmas 10.2, 8.2, and 7.10. ■

Theorem 10.4 (Countable Models)

Every satisfiable branch has a countable model.

Proof Let A be a satisfiable branch. Without loss of generality we assume that A is sufficiently pure. Hence $A \in \Gamma_C$. By Lemmas 10.2 and 8.2 we have a complete evident set E such that $A \subseteq E$. By Lemma 7.10 we have a countable model for E and hence for A . ■

Theorem 10.5 (Countable Model Existence)

Every evident branch has a countable model.

Proof Let E be an evident branch. By Lemma 7.10 we know that E is satisfiable. By Theorem 10.4 we know that E has a countable model. ■

11 Decidability

The tableau system \mathcal{R} defined in §9 yields a procedure that decides the satisfiability of three substantial fragments of EFO. Starting with the initial branch, the procedure applies tableau rules until it reaches a branch that contains \perp or cannot be extended with the tableau rules. The procedure returns “satisfiable” if it arrives at a terminal branch that does not contain \perp , and “unsatisfiable” if it finds a refutation. There are branches on which the procedure does not terminate (e.g., $\{\forall x. fx \neq x\}$). We first establish the partial correctness of the procedure.

Proposition 11.1 (Verification Soundness) Let A be a finite branch that does not contain \perp and cannot be extended with \mathcal{R} . Then A is evident and has a finite model.

Proof The evidence of a branch as specified is easily verified. The existence of a finite model follows with Theorem 7.9. ■

Proposition 11.2 (Refutation Soundness)

Every refutable branch is unsatisfiable.

Proof Let the branches A_1, \dots, A_n be obtained from a satisfiable branch A by application of a rule of \mathcal{R} . It suffices to show that one of the branches A_1, \dots, A_n is satisfiable. For \mathcal{T}_\neg this follows from the fact that the implication $x \wedge \neg x \rightarrow \perp$ is valid. For $\mathcal{T}_{\neg\wedge}$ the validity of $\neg(x \wedge y) \rightarrow \neg x \vee \neg y$ suffices, and for \mathcal{T}_{FE} the validity of $f \neq g \rightarrow \exists x. fx \neq gx$ does the job. The soundness of the other rules follows with similar arguments. ■

For the termination of the procedure we consider the relation $A \rightarrow A'$ that holds if A and A' are branches such that $\perp \notin A \subsetneq A'$ and A' can be obtained from A by applying a rule of \mathcal{R} . We say that \mathcal{R} **terminates** on a set Δ of branches if there is no infinite derivation $A \rightarrow A' \rightarrow A'' \rightarrow \dots$ such that $A \in \Delta$.

Proposition 11.3 Let \mathcal{R} terminate on a set Δ of finite branches. Then satisfiability of the branches in Δ is decidable and every satisfiable branch in Δ has a finite model.

Proof Follows with Propositions 11.2 and 11.1 and Theorem 7.9. ■

The decision procedure depends on the normalization operator employed with \mathcal{R} . A normalization operator that yields β -normal forms provides for all termination results proven in this section. Note that the tableau system applies the normalization operator only to applications st where s and t are both normal and t has type ι if it is not a variable. Hence at most one β -reduction is needed

for normalization if s and t are β -normal. Moreover, no α -renaming is needed if the bound variables are chosen differently from the free variables. For clarity, we continue to work with an abstract normalization operator and state a further condition:

N5 The least relation \succ on terms such that

1. $as_1 \dots s_n \succ s_i$ if $i \in \{1, \dots, n\}$
2. $s \succ [sx]$ if $s : \sigma\tau$ and $x : \sigma$

terminates on normal terms.

11.1 Pure Disequations

A type is **pure** if it does not contain o . A term is **pure** if the type of every name occurring in it (bound or unbound) is pure. An equation $s = t$ or disequation $s \neq t$ is **pure** if s and t are pure terms.

Proposition 11.4 (Pure Termination) Let the normalization operator satisfy N5. Then \mathcal{R} terminates on finite branches containing only pure disequations.

Proof Let $A \rightarrow A_1 \rightarrow A_2 \rightarrow \dots$ be a possibly infinite derivation that issues from a finite branch containing only pure disequations. Then no other rules but possibly \mathcal{T}_{DEC} , \mathcal{R}_{FE} , and \mathcal{T}_{\neq} apply and thus no A_i contains a formula that is not \perp or a pure disequations (using S5). Using N5 it follows that the derivation is finite. ■

We now know that the validity of pure equations is decidable, and that the invalidity of pure equations can be demonstrated with finite interpretations (Proposition 11.1). Both results are well-known [6, 10], but it is remarkable that we obtain them with different proofs and as a byproduct.

Example 11.5 \mathcal{R} does not terminate on branches that contain pure equations and pure disequations. We assume the typing $F : (\iota)\iota$ and $f : \iota\iota$.

$F(\lambda x.F(fx)) = a, F(fa) \neq a$	initial branch
$F(\lambda x.F(fx)) \neq F(fa), a \neq F(fa)$	\mathcal{T}_{CON}
$(\lambda x.F(fx)) \neq fa$	\mathcal{T}_{DEC}
$F(fb) \neq fab$	\mathcal{R}_{FE}
$F(\lambda x.F(fx)) \neq F(fb), a \neq F(fb)$	\mathcal{T}_{CON}
...	

The non-termination depends on the fact that the positive equation is not first-order. We can prove termination if we constrain the positive equations to be first-order, that is, to contain only variables whose type has the form $\iota \dots \iota$. This

restriction yields \mathcal{R}_{FE} non-applicable. Admitting quantifier-free formulas with variables whose types have the form $\sigma_1 \dots \sigma_n o$ where $n \geq 0$ and $\sigma_1, \dots, \sigma_n$ are pure types also preserves termination. \square

11.2 Bernays-Schönfinkel-Ramsey Formulas

It is well-known that satisfiability of Bernays-Schönfinkel-Ramsey formulas (first-order $\exists^* \forall^*$ -prenex formulas without functions) is decidable and the fragment has the finite model property [4]. We reobtain this result by showing that \mathcal{R} terminates for the respective fragment. We call a type **BSR** if it is ι or o or has the form $\iota \dots \iota o$. We call an EFO formula s **BSR** if it satisfies two conditions:

1. The type of every variable that occurs in s is BSR.
2. \forall_i does not occur below a negation in s .

For simplicity, our BSR formulas don't provide for outer existential quantification. We need one more condition for the normalization operator:

N6 If $s : \iota o$ is BSR and $x : \iota$, then $[sx]$ is BSR.

Proposition 11.6 (BSR Termination) Let the normalization operator satisfy N5 and N6. Then \mathcal{R} terminates on finite branches containing only BSR formulas.

Proof Let $A \rightarrow A_1 \rightarrow A_2 \rightarrow \dots$ be a possibly infinite derivation that issues from a finite branch containing only BSR formulas. Then $\mathcal{R}_{\neg\forall}$ and \mathcal{R}_{FE} are not applicable and all A_i contain only BSR formulas (using N6). Furthermore, at most one new variable is introduced. Since all terms of type ι are variables, there is only a finite supply. Using N5 it follows that the derivation is finite. \blacksquare

11.3 Lambda-Free Formulas

In [3] we study lambda- and quantifier-free EFO and show that the concomitant subsystem of \mathcal{R} terminates on finite branches. The result extends to lambda-free branches containing quantifiers (e.g., $\{\forall_i f\}$).

Proposition 11.7 (Lambda-Free Termination) Let the normalization operator satisfy $[s] = s$ for every lambda-free EFO term s . Then \mathcal{R} terminates on finite lambda-free branches.

Proof An application of \mathcal{R}_{FE} disables a disequation $s \neq_{\sigma\tau} t$ and introduces new subterms as follows: a variable $x : \sigma$, two terms $sx : \tau$ and $tx : \tau$, and two formulas $sx = tx$ and $sx \neq tx$. Since the types of the new subterms are smaller than the type of s and t , and the new subterms introduced by the other rules always have type o or ι , no derivation can employ \mathcal{R}_{FE} infinitely often.

Let $A \rightarrow A_1 \rightarrow A_2 \rightarrow \dots$ be a possibly infinite derivation that issues from a finite lambda-free branch and does not employ \mathcal{R}_{FE} . It suffices to show that the derivation is finite. Observe that no new subterms of the form $\forall_t s$ are introduced. Hence only finitely many new subterms of type ι are introduced. Consequently, only finitely many new subterms of type o are introduced. Hence the derivation is finite. ■

12 Conclusion

In this paper we have shown that the EFO fragment of Church's type theory enjoys the characteristic properties of first-order logic. We have devised a complete tableau system that comes with a new treatment of equality (confrontation) and a novel subterm restriction for the universal quantifier (discriminating terms). The tableau system decides lambda-free formulas, Bernays-Schönfinkel-Ramsey formulas, and equations between pure lambda terms.

References

- [1] Peter B. Andrews. Classical type theory. In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, volume 2, chapter 15, pages 965–1007. Elsevier Science, 2001.
- [2] Chad E. Brown. *Automated Reasoning in Higher-Order Logic: Set Comprehension and Extensionality in Church's Type Theory*. College Publications, 2007.
- [3] Chad E. Brown and Gert Smolka. Terminating tableaux for the basic fragment of simple type theory. In M. Giese and A. Waaler, editors, *TABLEAUX 2009*, volume 5607 of *LNCS (LNAI)*, pages 138–151. Springer, 2009.
- [4] Egon Börger, Erich Grädel, and Yuri Gurevich. *The Classical Decision Problem*. Springer, 1997.
- [5] Melvin Fitting. *First-Order Logic and Automated Theorem Proving*. Springer, 1996.
- [6] Harvey Friedman. Equality between functionals. In R. Parikh, editor, *Proc. Logic Colloquium 1972-73*, volume 453 of *Lectures Notes in Mathematics*, pages 22–37. Springer, 1975.
- [7] J. R. Hindley. *Basic Simple Type Theory*, volume 42 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1997.

- [8] Dag Prawitz. Hauptsatz for higher order logic. *J. Symb. Log.*, 33:452–457, 1968.
- [9] Raymond M. Smullyan. *First-Order Logic*. Springer, 1968.
- [10] Richard Statman. Completeness, invariance and lambda-definability. *J. Symb. Log.*, 47(1):17–26, 1982.