A Sound and Complete Proof System for STTwU*

William M. Farmer†
McMaster University

September 15, 2004

Abstract

STTwU is a very simple version of simple type theory that admits undefined terms and statements about definedness. This paper gives a Hilbert-style proof system for STTwU and proves that it is sound and complete for the general model semantics for STTwU.

1 Introduction

STTwU is a very simple version of simple type theory that admits undefined terms and statements about definedness [6]. (STTwU is short for Simple Type Theory with Undefinedness.) $\mathbf{A_u}$ is a Hilbert-style proof system for STTwU defined below. It is a modification of the proof system $\mathbf{A}$ for STT given in [5] which is based on P. Andrews' proof system [1, 2] for $\mathcal{Q}_0$, an elegant version of Church's type theory. $\mathbf{A_u}$ is closely related to the proof systems for the undefinedness logics **PF** [3] and $\mathbf{PF}^*$ [4].

We prove that $\mathbf{A_u}$ is sound and complete with respect to the general models semantics for STTwU. The completeness proof is very similar to the completeness proofs for **PF** and $\mathbf{PF}^*$, which are derived from Andrews' proof of the Henkin completeness theorem [7] for $\mathcal{Q}_0$.

We assume the reader is familiar with the definitions given in [6].

*Published as Technical Report No. CAS-04-01-WF, 8 pp., McMaster University, 2004.

†Address: Department of Computing and Software, McMaster University, 1280 Main Street West, Hamilton, Ontario L8S 4K1, Canada. E-mail: `wmfarmer@mcmaster.ca`.

2 General Models

A *general structure* for a language $L = (\mathcal{C}, \tau)$ of STTwU is a pair $M = (\mathcal{D}, I)$ where:

(1) $\mathcal{D} = \{D_\alpha : \alpha \in \mathcal{T}\}$ is a set of nonempty domains (sets).

(2) $D_* = \{\text{T}, \text{F}\}$.

(3) For $\alpha, \beta \in \mathcal{T}$, $D_{\alpha \rightarrow \beta}$ is some nonempty set of *total* functions from D_α to D_β if $\beta = *$ and some nonempty set of *partial and total* functions from D_α to D_β if $\beta \neq *$.

(4) I maps each $c \in \mathcal{C}$ to a member of $D_{\tau(c)}$.

M is a *general model*[1] for L if there is a binary function V^M that satisfies the same conditions as the valuation function for a standard model (see [6]). A general model is thus the same as a standard model except that the function domains of the model may not be "fully inhabited". Hence every standard model for L is also a general model for L.

Let $\Gamma \cup \{A\}$ be a set of formulas of L. A is *valid* in M, written $M \models A$, if $V^M_\varphi(A) = \text{T}$ for all variable assignments φ into M. M is a *general model* for Γ if $M \models B$ for all $B \in \Gamma$. A is *valid in the general sense* if $M \models A$ for every general model M for L.

3 The Proof System

$\mathbf{A_u}$ is defined relative to a STTwU language $L = (\mathcal{C}, \tau)$. It consists of the following sixteen axiom schemas and two rules of inference:

A1 (Truth Values)

$$\forall\, f : (* \rightarrow *) \;.\; (f(\mathsf{T}) \wedge f(\mathsf{F})) \Leftrightarrow (\forall\, x : * \;.\; f(x)).$$

A2 (Leibniz' Law)

$$\forall\, x, y : \alpha \;.\; (x = y) \Rightarrow (\forall\, p : (\alpha \rightarrow *) \;.\; p(x) \Leftrightarrow p(y)).$$

A3 (Extensionality)

$$\forall\, f, g : (\alpha \rightarrow \beta) \;.\; (f = g) \Leftrightarrow (\forall\, x : \alpha \;.\; f(x) \simeq g(x)).$$

[1]The notion of a "general model" was introduced by L. Henkin in [7].

A4 (Beta-Reduction)

$$A_\alpha\downarrow \Rightarrow (\lambda\, x : \alpha \,.\, B_\beta)(A_\alpha) \simeq B_\beta[(x : \alpha) \mapsto A_\alpha]$$

provided A_α is free for $(x : \alpha)$ in B_β.

A5 (Equality and Quasi-Quality)

$$A_\alpha\downarrow \Rightarrow (B_\alpha\downarrow \Rightarrow (A_\alpha \simeq B_\alpha) \simeq (A_\alpha = B_\alpha)).$$

A6 (Expressions of Type $*$ are Defined)

$$A_*\downarrow .$$

A7 (Variables are Defined)

$$(x : \alpha)\downarrow \quad \text{where } x \in \mathcal{V} \text{ and } \alpha \in \mathcal{T}.$$

A8 (Constants are Defined)

$$c\downarrow \quad \text{where } c \in \mathcal{C}.$$

A9 (Function Abstractions are Defined)

$$(\lambda\, x : \alpha \,.\, B_\beta)\downarrow$$

A10 (Improper Function Application)

$$(F_{\alpha\to\beta}\uparrow \vee A_\alpha\uparrow) \Rightarrow F_{\alpha\to\beta}(A_\alpha)\uparrow \quad \text{where } \beta \neq *.$$

A11 (Improper Predicate Application)

$$(F_{\alpha\to *}\uparrow \vee A_\alpha\uparrow) \Rightarrow \neg F_{\alpha\to *}(A_\alpha).$$

A12 (Improper Equality)

$$(A_\alpha\uparrow \vee B_\alpha\uparrow) \Rightarrow \neg(A_\alpha = B_\alpha).$$

A13 (Proper Definite Description of Type $\alpha \neq *$)

$$(\exists\,!\, x : \alpha \,.\, A_*) \Rightarrow ((\mathrm{I}\, x : \alpha \,.\, A_*)\downarrow \wedge A_*[(x : \alpha) \mapsto (\mathrm{I}\, x : \alpha \,.\, A_*)])$$

where $\alpha \neq *$ and provided $(\mathrm{I}\, x : \alpha \,.\, A_*)$ is free for $(x : \alpha)$ in A_*.

A14 (Improper Definite Description of Type $\alpha \neq *$)

$$\neg(\exists\,!\,x : \alpha \,.\, A_*) \Rightarrow (\mathrm{I}\,x : \alpha \,.\, A_*)\!\uparrow \quad \text{where } \alpha \neq *.$$

A15 (Proper Definite Description of Type $*$)

$$(\exists\,!\,x : * \,.\, A_*) \Rightarrow A_*[(x : *) \mapsto (\mathrm{I}\,x : * \,.\, A_*)]$$

provided $(\mathrm{I}\,x : * \,.\, A_*)$ is free for $(x : *)$ in A_*.

A16 (Improper Definite Description of Type $*$)

$$\neg(\exists\,!\,x : * \,.\, A_*) \Rightarrow \neg(\mathrm{I}\,x : * \,.\, A_*).$$

R1 (Modus Ponens) From A_* and $A_* \Rightarrow B_*$ infer B_*.

R2 (Quasi-Equality Substitution) From $A_\alpha \simeq B_\alpha$ and C_* infer the result of replacing one occurrence of A_α in C_* by an occurrence of B_α, provided that the occurrence of A_α in C_* is not immediately preceded by λ.

A *proof* of a formula A in $\mathbf{A_u}$ is a finite sequence of formulas of L, ending with A, such that each member in the sequence is an instance of an axiom schema of $\mathbf{A_u}$ or is inferred from preceding formulas in the sequence by a rule of inference of $\mathbf{A_u}$. A *theorem* of $\mathbf{A_u}$ is a formula for which there is a proof in $\mathbf{A_u}$.

Let Γ be a set of formulas of L. A *proof* of a formula A from Γ in $\mathbf{A_u}$ is a finite sequence $\pi_1{}^\frown\pi_2$ of formulas, ending with A, such that π_1 is a proof in $\mathbf{A_u}$ and each member D of π_2 satisfies at least one of the following conditions:

(1) $D \in \Gamma$.

(2) D is a member of π_1 (and hence a theorem of $\mathbf{A_u}$).

(3) D is inferred from preceding members of π_2 by R1.

(4) D is inferred from two preceding members $A_\alpha \simeq B_\alpha$ and C_* of π_2 by R2, provided that the occurrence of A_α in C_* is not in a subexpression $\lambda\,x : \beta \,.\, E_\gamma$ of C_* where $(x : \beta)$ is free in a member of Γ and free in $A_\alpha \simeq B_\beta$.

We write $\Gamma \vdash A$ to mean there is a proof of A from Γ in $\mathbf{A_u}$. ($\vdash A$ is written instead of $\emptyset \vdash A$.) Clearly, A is a theorem of $\mathbf{A_u}$ iff $\vdash A$. The next two theorems follow immediately from the definition above.

Theorem 1 (R1′) *If $\Gamma \vdash A_*$ and $\Gamma \vdash A_* \Rightarrow B_*$, then $\Gamma \vdash B_*$.*

Theorem 2 (R2′) *If $\Gamma \vdash A_\alpha \simeq B_\alpha$ and $\Gamma \vdash C_*$, then $\Gamma \vdash D_*$, where D_* is the result of replacing one occurrence of A_α in C_* by an occurrence of B_α, provided that the occurrence of A_α in C_* is not immediately preceded by λ or in a subexpression $\lambda\, x : \beta \,.\, E_\gamma$ of C_* where $(x : \beta)$ is free in a member of Γ and free in $A_\alpha \simeq B_\alpha$.*

4 Basic Metatheorems

Theorem 3 (Beta-Reduction Rule) *If $\Gamma \vdash A_\alpha\!\downarrow$ and $\Gamma \vdash C_*$, then $\Gamma \vdash D_*$, where D_* is the result of replacing one occurrence of $(\lambda\, x : \alpha \,.\, B_\beta)(A_\alpha)$ in C_* by an occurrence of $B_\beta[(x : \alpha) \mapsto A_\alpha]$, provided A_α is free for $(x : \alpha)$ in B_β and the occurrence of $(\lambda\, x : \alpha \,.\, B_\beta)(A_\alpha)$ in C_* is not in a subexpression $\lambda\, y : \gamma \,.\, E_\delta$ of C_* where $(y : \gamma)$ is free in a member of Γ and free in $(\lambda\, x : \alpha \,.\, B_\beta)(A_\alpha)$.*

Proof Follows immediately from A4, R1′, and R2′. □

Lemma 1 *If $\Gamma \vdash A_\alpha\!\downarrow$, then $\Gamma \vdash A_\alpha \simeq A_\alpha$.*

Proof We obtain $\Gamma \vdash (\lambda\, x : \alpha \,.\, x)(A_\alpha) \simeq A_\alpha$ by applying R1′ to the hypothesis and an instance of A4. The conclusion of the lemma then follows by the Beta-Reduction Rule. □

Corollary 1 $\vdash \mathsf{T}$.

Proof By the definition of T, A9, and Lemma 1. □

Lemma 2 *If $\Gamma \vdash A_\alpha\!\downarrow$ and $\Gamma \vdash B_\alpha\!\downarrow$, then $\Gamma \vdash A_\alpha \simeq B_\alpha$ iff $\Gamma \vdash A_\alpha = B_\alpha$.*

Proof

($\Rightarrow$): Follows immediately from A5, R1′, and R2′.

($\Leftarrow$): $\Gamma \vdash (A_\alpha \simeq B_\alpha) \simeq (A_\alpha = B_\alpha)$ by the first two hypotheses, A5, and R1′. $\vdash (A_\alpha \simeq B_\alpha) \simeq (A_\alpha \simeq B_\alpha)$ by A6 and Lemma 1. We obtain $\Gamma \vdash (A_\alpha = B_\alpha) \simeq (A_\alpha \simeq B_\alpha)$ by applying R2′ to these two statements. The conclusion of the lemma then follows by applying R2$'$ to this statement and $\Gamma \vdash A_\alpha = B_\alpha$. $\Box$

As a result of A6 and Lemma 2, a quasi-equality $A_* \simeq B_*$ and an equality $A_* = B_*$ are completely interchangeable in $\mathbf{A_u}$.

Theorem 4 (Universal Instantiation) *If* $\Gamma \vdash \forall\, x : \alpha \;.\; B_*$ *and* $\Gamma \vdash A_\alpha$, *then* $\Gamma \vdash B_*[(x:\alpha) \mapsto A_\alpha]$, *provided* A_α *is free for* $(x : \alpha)$ *in* B_*.

Proof $\Gamma \vdash \lambda\, x : \alpha \;.\; B_* = \lambda\, x : \alpha \;.\; \mathsf{T}$ by the first hypothesis, the definition of $\forall$, A9, and the Beta-Reduction Rule. $\Gamma \vdash (\lambda\, x : \alpha \;.\; B_*)(A_\alpha) \simeq B_*[(x : \alpha) \mapsto A_\alpha]$ by the second hypothesis, A4, and R1$'$. We obtain $\Gamma \vdash (\lambda\, x : \alpha \;.\; \mathsf{T})(A_\alpha) \simeq B_*[(x : \alpha) \mapsto A_\alpha]$ from these two statements by Lemma 2 and R2$'$. Then $\Gamma \vdash \mathsf{T} \simeq B_*[(x : \alpha) \mapsto A_\alpha]$ by the second hypothesis and the Beta-Reduction Rule. The conclusion of the theorem is obtained by applying R2$'$ to this statement and the conclusion of Corollary 1. $\Box$

Universal Instantiation is needed to instantiate axiom schemas A1–3.

Theorem 5 (Tautology Theorem) *If* A *is a tautological consequence of* $B_1, \ldots, B_n$ *and* $\Gamma \vdash B_1, \ \ldots, \ \Gamma \vdash B_n$ *for* $n \geq 0$, *then* $\Gamma \vdash A$.

Proof Lemma 2 and Universal Instantiation enable the theorem to be proved by an argument very similar to the proof of Theorem 5234 in [2]. $\Box$

Proposition 1 $\vdash (A_\alpha = B_\alpha) \Rightarrow (A_\alpha \simeq B_\alpha)$.

Proof Follows from the definition of $\simeq$ and the Tautology Theorem. $\Box$

Theorem 6 (Deduction Theorem) *If* $\Gamma \cup \{A\} \vdash B$, *then* $\Gamma \vdash A \Rightarrow B$.

Proof Similar to the proof of Theorem 5240 in [2]. $\Box$

5 Soundness and Completeness

Let $\Gamma \cup \{A\}$ be a set of formulas of L. Γ is *consistent* if there is no proof of F from Γ.

Theorem 7 (Soundness Theorem) *If* $\Gamma \vdash A$, *then* $M \models A$ *for every general model* M *for* Γ.

Proof Each instance of each axiom schema of $\mathbf{A_u}$ is valid in the general sense, and R1 and R2 preserve validity in every general model for L. The theorem then follows from the Deduction Theorem. See the proof of Theorem 5402 in [2] for details. □

Theorem 8 (Consistency Theorem) *If Γ has a general model, then Γ is consistent.*

Proof Let M be a general model for Γ. Assume that Γ is inconsistent, i.e., that $\Gamma \vdash \mathsf{F}$. Then, by the Soundness Theorem, $M \models \mathsf{F}$, and so $V_\varphi^M(\mathsf{F}) = \textsc{t}$ (for any variable assignment φ), which contradicts the definition of a general model. □

Theorem 9 (Henkin's Theorem for STTwU) *If Γ is a consistent set of sentences of L, then Γ has a general model.*

Proof Similar to the proof of Theorem 7.2 in [3]. The proof requires the axiom schemas A6–16 that concern definedness. □

Theorem 10 (Henkin's Completeness Theorem for STTwU) *Let Γ be a set of sentences of L. If $M \models A$ for every general model M for Γ, then $\Gamma \vdash A$.*

Proof Assume $M \models A$ for every general model M for Γ, and let B be the universal closure of A. Then $M \models B$ for every general model M for Γ. Suppose $\Gamma \cup \{\neg B\}$ is consistent. Then, by Henkin's Theorem for STTwU, there is a general model M_0 for $\Gamma \cup \{\neg B\}$, and so $M_0 \models \neg B$. Since M_0 is also a general model for Γ, $M_0 \models B$. From this contradiction it follows that $\Gamma \cup \{\neg B\}$ is inconsistent. Hence $\Gamma \vdash B$ by the Deduction Theorem and the Tautology Theorem. Therefore, $\Gamma \vdash A$ by Universal Instantiation and A7. □

References

[1] P. B. Andrews. A reduction of the axioms for the theory of propositional types. *Fundamenta Mathematicae*, 52:345–350, 1963.

[2] P. B. Andrews. *An Introduction to Mathematical Logic and Type Theory: To Truth through Proof, Second Edition.* Kluwer, 2002.

[3] W. M. Farmer. A partial functions version of Church's simple theory of types. *Journal of Symbolic Logic*, 55:1269–91, 1990.

[4] W. M. Farmer. A simple type theory with partial functions and subtypes. *Annals of Pure and Applied Logic*, 64:211–240, 1993.

[5] W. M. Farmer. The seven virtues of simple type theory. SQRL Report No. 18, McMaster University, 2003.

[6] W. M. Farmer. Formalizing undefinedness arising in calculus. In D. Basin and M. Rusinowitch, editors, *Automated Reasoning—IJCAR 2004*, volume 3097 of *Lecture Notes in Computer Science*, pages 475–489. Springer-Verlag, 2004.

[7] L. Henkin. Completeness in the theory of types. *Journal of Symbolic Logic*, 15:81–91, 1950.