Intelligible Formal Proofs

Dem.

$\vdash . *2{\cdot}08 . \quad \supset \vdash : \phi z \supset \psi z . \supset . \phi z \supset \psi z$ (1)

$\vdash . (1) . *9{\cdot}1 . \quad \supset \vdash : (\exists y) : \phi z \supset \psi z . \supset . \phi y \supset \psi z$ (2)

$\vdash . (2) . *9{\cdot}1 . \quad \supset \vdash :. (\exists x) :. (\exists y) : \phi x \supset \psi x . \supset . \phi y \supset \psi z$ (3)

$\vdash . (3) . *9{\cdot}13 . \quad \supset \vdash :: (z) :: (\exists x) :. (\exists y) : \phi x \supset \psi x . \supset . \phi y \supset \psi z$ (4)

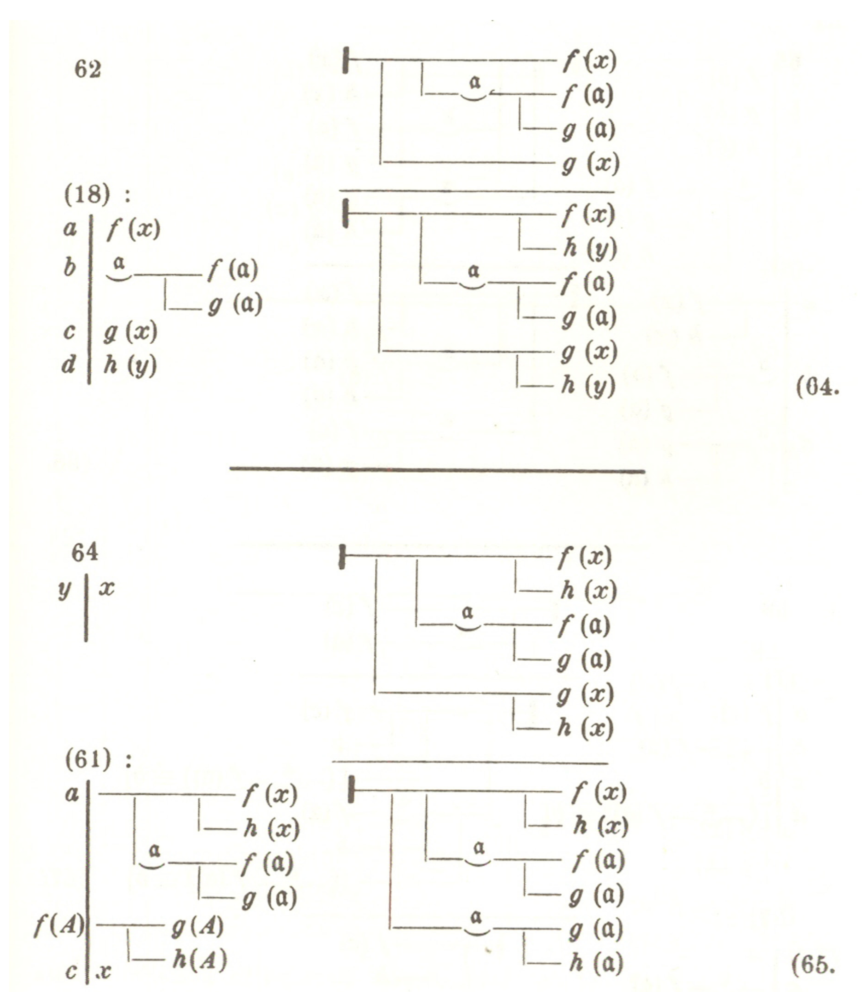
$[(4).(*9{\cdot}06)] \quad \vdash :: (z) :: (\exists x) :. \phi x \supset \psi x . \supset : (\exists y) . \phi y \supset \psi z$ (5)

$[(5).(*1{\cdot}01.*9{\cdot}08)] \quad \vdash :. (\exists x) . \sim (\phi x \supset \psi x) : \vee : (z) : (\exists y) . \sim \phi y \vee \psi z$ (6)

$[(6).(*9{\cdot}08)] \quad \vdash :. (\exists x) . \sim (\phi x \supset \psi x) : \vee : (\exists y) . \sim \phi y . \vee . (z) . \psi z$ (7)

$[(7).(*1{\cdot}01)] \quad \vdash :. (x) . \phi x \supset \psi x . \supset : (y) . \phi y . \supset . (z) . \psi z$

Principia Mathematica (1910), Alfred North Whitehead and Bertrand Russell



Begriffsschrift (1879), Gottlob Frege

1	$u \subseteq v \,\&\, w = v \setminus u$	Assume
2	$u \subseteq v$	&EL: 1
3	$w = v \setminus u$	&ER: 1
4	$x_1 \in u$	Assume
5	$(\forall x)(x \in u \to x \in v)$	DefE(⊆): 2
6	$x_1 \in u \to x_1 \in v$	∀E: 5
7	$x_1 \in v$	→E: 6,4
8	$x_1 \in w$	Assume
9	$x_1 \in v \setminus u$	=E: 8,3
10	$x_1 \in v \,\&\, x_1 \notin u$	DefE(\): 9
11	$x_1 \notin u$	&ER: 10
12	$\perp$	⊥I: 4,11
13	$x_1 \notin w$	¬I: 12
14	$x_1 \in v \,\&\, x_1 \notin w$	&I: 7,13
15	$x_1 \in v \setminus w$	DefI(\): 14
16	$x_1 \in v \setminus w$	Assume
17	$x_1 \notin u$	Assume
18	$x_1 \in v \,\&\, x \notin w$	DefE(\): 16
19	$x_1 \in v$	&EL: 18
20	$x_1 \notin w$	&ER: 18
21	$x_1 \in v \,\&\, x_1 \notin u$	&I: 19,17
22	$x_1 \in v \setminus u$	DefI(\): 21
23	$(\forall z)(z \in w \leftrightarrow z \in v \setminus u)$	DefE(Ext): 3
24	$z_1 \in w \leftrightarrow z_1 \in v \setminus u$	∀E: 23
25	$z_1 \in v \setminus u$	Assume
26	$z_1 \in w$	↔EL: 24,25
27	$z_1 \in w$	Assume
28	$z_1 \in v \setminus u$	↔ER: 24,27
29	$z_1 \in v \setminus u \leftrightarrow z_1 \in w$	↔I: 26,28
30	$(\forall z)(z \in v \setminus u \leftrightarrow z \in w)$	∀I: 29
31	$v \setminus u = w$	DefI(Ext): 30
32	$x_1 \in w$	=E: 22,31
33	$\perp$	⊥I: 32,13
34	$x_1 \in u$	¬E: 33
35	$x_1 \in u \leftrightarrow x_1 \in v \setminus w$	↔I: 15,34
36	$(\forall x)(x \in u \leftrightarrow x \in v \setminus w)$	∀I: 35
37	$u = v \setminus w$	DefI(Ext): 36
38	$(u \subseteq v \,\&\, w = v \setminus u) \to u = v \setminus w$	→I: 37
39	$(\forall z)((u \subseteq v \,\&\, z = v \setminus u) \to u = v \setminus z)$	∀I: 38
40	$(\forall y)(\forall z)((u \subseteq y \,\&\, z = y \setminus u) \to u = y \setminus z)$	∀I: 39
41	$(\forall x)(\forall y)(\forall z)((x \subseteq y \,\&\, z = y \setminus x) \to x = y \setminus z)$	∀I: 40

1	$u \subseteq v$	Assume
2	$w = v \setminus u$	Assume
3	$x_1 \in u$	Assume
4	$x_1 \in v$	DefE(⊆): 1,3
5	$x_1 \in w$	Assume
6	$x_1 \in v \setminus u$	=E: 5,2
7	$x_1 \notin u$	DefE(\): 6
8	$\perp$	⊥I: 3,7
9	$x_1 \notin w$	¬I: 8
10	$x_1 \in v \setminus w$	DefI(\): 4,9
11	$x_1 \in v \setminus w$	Assume
12	$x_1 \notin u$	Assume
13	$x_1 \in v$	DefE(\): 11
14	$x_1 \notin w$	DefE(\): 11
15	$x_1 \in v \setminus u$	DefI(\): 13,12
16	$x_1 \in w$	=E: 15,2
17	$\perp$	⊥I: 16,14
18	$x_1 \in u$	¬E: 17
19	$u = v \setminus w$	ExtI: 10,18
20	$(\forall x, y, z)((x \subseteq y \,\&\, z = y \setminus x) \to x = y \setminus z)$	∀(→)I: 19

Abbreviating Notions

Abbreviated Series of Quantifiers

Consecutive universally quantified variables are attached to a single quantifier and instantiated in a single step.

Assumption/Goal Generation for Universally-Quantified Conditional

Subderivation is automatically created with all conjuncts in the antecedent presented as assumptions and the consequent as its goal.

Abbreviation of Extensionality Introduction

Subderivations are automatically generated with an arbitrary variable.

Abbreviation of Subset Elimination

Expansion of the definition of subset is not required; conclusion can be made from subset relation and statement of membership.

Piecewise Definition Elimination

Only the part of the definition being utilized is extracted.

WHY?

Establishing the legitimacy of a theorem from within a formal system is done by means of a formal proof. Such proofs, however, can be lengthy and enigmatic, making them impractical in an educational context. Formal abbreviating notions serve to aid our progress in mathematics in two fundamental ways:

1. Formal proofs become shorter and more intelligible to the reader. One is able to grasp the overall structure of the proof more easily and is not led astray by tedious proof steps that do not directly contribute to one's understanding of the proof. Altering the presentation of a formal proof to be more transparent to human understanding without affecting the content of the proof provides mathematicians with a rigorous framework for establishing meaningful results while avoiding the pitfalls of cumbersome notation.

2. Formal proofs can be used in an educational context to promote student-understanding of established mathematical results. Informal proofs are often not suitable for classroom study as mathematicians, for the sake of brevity, often omit steps in reasoning and presuppose the reader's ability to follow the argument. Formal proofs have a similar fate as the notation can become overwhelming and can prevent the student from understanding the key ideas of the proof. Abbreviated formal proofs provide students with a proof presentation that includes all essential steps in reasoning without cluttering the proof space with excessive notation.

AProS
automated proof search

This project was pursued within the framework of the AProS project, a multifaceted program involving a unique integration of automated proof generation and computer-based instruction for students. The program includes:

- a Proof Generator that searches for natural deduction proofs in first-order logic and set theory
- a Proof Lab for formal proof construction in an interactive environment
- a Proof Tutor to provide student assistance in proof formulation
- online courses titled Logic & Proofs, and Functions & Computations

The AProS Project is supported by a grant from the National Science Foundation and is directed by Wilfried Sieg.

Project By:
Adam Conkey
MCS 2011
Mathematics, Philosophy
aconkey@andrew.cmu.edu

Advised By:
Wilfried Sieg
Professor of Philosophy
sieg@cmu.edu