

H A N D B O O K O F

Logic and Proof Techniques for Computer Science

S T E V E N G . K R A N T Z

Steven G. Krantz

Handbook of Logic and Proof Techniques for Computer Science

With 16 Figures

BIRKHÄUSER
BOSTON



SPRINGER
NEW YORK

Steven G. Krantz
Department of Mathematics
Washington University
One Brookings Drive
St. Louis, MO 63130
USA

Library of Congress Cataloging-in-Publication Data

Krantz, Steven G. (Steven George), 1951–

Handbook of logic and proof techniques for computer science / Steven G. Krantz.
p. cm.

Includes bibliographical references and index.

ISBN 0-8176-4220-X (alk. paper)

1. Computers. 2. Electronic data processing. I. Title.

QA76 .K723 2002

004—dc21

2001043153

CIP

Printed on acid-free paper.

© 2002 Birkhäuser Boston

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Birkhäuser Boston, c/o Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

ISBN 0-8176-4220-X

ISBN 3-7643-4220-X SPIN 10850279

Production managed by Louise Farkas; manufacturing supervised by Joe Quatela.

Typeset by the author in LaTeX2e.

Printed and bound by Maple-Vail Book Manufacturing Group, York, PA.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

Handbook of Logic and Proof Techniques for Computer Science

To little Hypatia, who doesn't seem to be very logical.

Preface

Logic is, and should be, the core subject area of modern mathematics. The blueprint for twentieth century mathematical thought, thanks to Hilbert and Bourbaki, is the axiomatic development of the subject. As a result, logic plays a central conceptual role. At the same time, mathematical logic has grown into one of the most recondite areas of mathematics. Most of modern logic is inaccessible to all but the specialist.

Yet there is a need for many mathematical scientists—not just those engaged in mathematical research—to become conversant with the key ideas of logic. *The Handbook of Mathematical Logic*, edited by Jon Barwise, is in point of fact a handbook written by logicians for other mathematicians. It was, at the time of its writing, encyclopedic, authoritative, and up-to-the-moment. But it was, and remains, a comprehensive and authoritative book for the *cognoscenti*. The encyclopedic *Handbook of Logic in Computer Science* by Abramsky, Gabbay, and Maibaum is a wonderful resource for the professional. But it is overwhelming for the casual user. There is need for a book that introduces important logic terminology and concepts to the working mathematical scientist who has only a passing acquaintance with logic. Thus the present work has a different target audience.

The intent of this handbook is to present the elements of modern logic, including many current topics, to the reader having only basic mathematical literacy. Certainly a college minor in mathematics is more than sufficient background to read this book. Specifically, courses in linear algebra, finite mathematics, and mathematical structures would be more than adequate preparation. From the computer science side, it would be good if the reader knew a programming language and had some exposure to issues of complexity and decidability. But all these prerequisites are primarily for motivation. This handbook is, to the extent possible, self-contained. It will be a compact and accessible reference.

This is not a textbook; it is a handbook. It contains very few proofs. What it does contain are definitions, examples, and discussion of all of the key ideas in basic logic. We also include cogent and self-contained in-

introductions to critical advanced topics, including Gödel's completeness and incompleteness theorems, methods of proof, cardinal and ordinal numbers, the continuum hypothesis, the axiom of choice, model theory, number systems and their construction, multi-valued logics, category theory, universal algebra, proof theory, fuzzy set theory, recursive functions, **NP**-completeness, decision problems, Boolean algebra, semantics, decision problems, and the word problem.

This book is intended to be a resource for the working mathematical scientist. The computer scientist or engineer or system scientist who must have a quick sketch of a key idea from logic will find it here in self-contained form, accessible to a quick read. In addition to critical terminology, notation, and ideas, references for further reading are provided. There is a thorough index, a glossary, a lexicon of notation, a guide to the literature, and an extensive bibliography.

There is no other book like this one on the subject of logic and its allied areas. This book is both a reference and a portal to further study of topics in logic. A scientist reading a technical tract in another field and encountering an unfamiliar term or concept from logic can turn to this volume and find a rapid introduction to the key points. The book will be a useful reference both for working scientists and for students.

Certainly computer science is one of the most active areas of modern scientific activity that uses logic. This book has been written with computer scientists in mind. Important ideas, such as recursion theory, decidability, independence, completeness, consistency, model theory, **NP**-completeness, and axiomatics are presented here in a form that is particularly accessible to computer scientists. Examples from computer science are provided whenever possible. A special effort has been made to cut through the mathematical formalism, difficult notation, and esoteric terminology that are typical of modern mathematical logic. The treatment of any key topic is quick, incisive, and to the point.

Although this is a handbook of logic, it is not strictly logical in nature. By this we mean that it is virtually impossible to present all of the topics of this great tapestry in a strictly logical order. For that reason, topics have been repeated or presented in unusual sequence when convenient for local use.

Birkhäuser engaged a number of experts to review various versions of this project and to help prepare it for publication. These reviewers patiently guided me regarding both form and substance. Their criticisms and remarks have been invaluable. Of course, responsibility for all remaining errors and malapropisms resides entirely with the author.

It is hoped that this work will stimulate the communication between computer science and mathematics, and also be a useful handbook for both fields. It is safe to say that computer science is becoming ever more mathematical and also that mathematics is becoming increasingly com-

fortable with the use of computers. This book should serve as a catalyst in both activities. It is both a touchstone for a first look at topics in logic and an invitation to further reading. We hope that it will awaken in others the fascination with logic that we have experienced for more than a quarter century.

Steven G. Krantz
St. Louis, Missouri

Contents

Preface

xvii

1	Notation and First-Order Logic	1
1.1	The Use of Connectives	1
1.1.1	Elementary Statements	1
1.1.2	Connectives	2
1.1.3	Redundancy of the Connectives	3
1.1.4	Additional Connectives	3
1.2	Truth Values and Truth Tables	4
1.2.1	Rules for Truth Values and Tables	4
1.2.2	Multivalued Logics	5
1.2.3	Modal Logic	6
1.2.4	Compound Sentences and Truth Values	6
1.2.5	Tautologies and Contradictions	7
1.2.6	Contrapositives	8
1.3	The Use of Quantifiers	8
1.3.1	“For All” and “There Exists”	8
1.3.2	Relations Between “For All” and “There Exists”	9
1.3.3	The Propositional and the Predicate Calculus	9
1.3.4	Derivability	10
1.3.5	Semantics and Syntax	11
1.3.6	A Consideration of First-Order Theories	11
1.3.7	Herbrand’s Theorem	12
1.3.8	An Example from Group Theory	13
1.4	Gödel’s Completeness Theorem	13
1.4.1	Provable Statements and Tautologies	13
1.4.2	Formulation of Gödel’s Completeness Theorem	14
1.4.3	Additional Terminology	15
1.4.4	Some More Formal Language	15
1.4.5	Other Formulations of Gödel Completeness	15

1.4.6	The Compactness Theorem	16
1.4.7	Tautological Implication and Provability	16
1.5	Second-Order Logic	17
1.5.1	Semantics	17
2	Semantics and Syntax	19
2.1	Elementary Symbols	20
2.1.1	Formal Systems (Syntax)	20
2.2	Well-Formed Formulas or wffs [Syntax]	21
2.3	Free and Bound Variables (Syntax)	21
2.4	The Semantics of First-Order Logic	21
2.4.1	Interpretations	21
2.4.2	Truth	22
2.4.3	First-Order Theories	22
2.4.4	A Proof System for First-Order Logic	22
2.4.5	Two Fundamental Theorems	23
3	Axiomatics and Formalism in Mathematics	25
3.1	Basic Elements	26
3.1.1	Undefinable Terms	26
3.1.2	Description of Sets	26
3.1.3	Definitions	26
3.1.4	Axioms	28
3.1.5	Lemmas, Propositions, Theorems, and Corollaries	29
3.1.6	Rules of Logic	30
3.1.7	Proofs	31
3.2	Models	31
3.2.1	Definition of Model	31
3.2.2	Examples of Models	31
3.2.3	Finite Model Theory	32
3.2.4	Minimality of Models	32
3.2.5	Universal Algebra	33
3.3	Consistency	33
3.3.1	Definition of Consistency	33
3.4	Gödel's Incompleteness Theorem	33
3.4.1	Introductory Remarks	33
3.4.2	Gödel's Theorem and Arithmetic	33
3.4.3	Formal Enunciation of Arithmetic	34
3.4.4	Some Standard Terminology	34
3.4.5	Enunciation of the Incompleteness Theorem	35
3.4.6	Church's Theorem	35
3.4.7	Additional Formulations of Incompleteness	36
3.4.8	Relative Consistency	36

3.5	Decidability and Undecidability	37
3.5.1	Introduction to Decidability	37
3.5.2	Recursive Equivalence; Degrees of Recursive Unsolvability	37
3.6	Independence	37
3.6.1	Introduction to Independence	37
3.6.2	Examples of Independence	38
4	The Axioms of Set Theory	39
4.1	Introduction	40
4.2	Axioms and Discussion	40
4.2.1	Axiom of Extensionality	40
4.2.2	Sum Axiom	40
4.2.3	Power Set Axiom	40
4.2.4	Axiom of Regularity	41
4.2.5	Axiom for Cardinals	41
4.2.6	Axiom of Infinity	41
4.2.7	Axiom Schema of Replacement	41
4.2.8	Axiom of Choice	42
4.3	Concluding Remarks	42
5	Elementary Set Theory	43
5.1	Set Notation	44
5.1.1	Elements of a Set	44
5.1.2	Set-Builder Notation	44
5.1.3	The Empty Set	44
5.1.4	Universal Sets and Complements	45
5.1.5	Set-Theoretic Difference	45
5.1.6	Ordered Pairs; the Product of Two Sets	46
5.2	Sets, Subsets, and Elements	46
5.2.1	The Elements of a Set	46
5.2.2	Venn Diagrams	47
5.3	Binary Operations on Sets	48
5.3.1	Intersection and Union	48
5.3.2	Properties of Intersection and Union	50
5.3.3	Other Set-Theoretic Operations	50
5.4	Relations and Equivalence Relations	51
5.4.1	What Is a Relation?	51
5.4.2	Partial and Full Orderings	51
5.5	Equivalence Relations	52
5.5.1	What Is an Equivalence Relation?	52
5.5.2	Equivalence Classes	52

5.5.3	Examples of Equivalence Relations and Classes	53
5.5.4	Construction of the Rational Numbers	54
5.6	Number Systems	55
5.7	Functions	56
5.7.1	What Is a Function?	56
5.7.2	Examples of Functions	56
5.7.3	One-to-One or Univalent	57
5.7.4	Onto or Surjective	58
5.7.5	Set-Theoretic Isomorphisms	59
5.8	Cardinal Numbers	59
5.8.1	Comparison of the Sizes of Sets	59
5.8.2	Cardinality and Cardinal Numbers	60
5.8.3	An Uncountable Set	61
5.8.4	Countable and Uncountable	63
5.8.5	Comparison of Cardinalities	64
5.8.6	The Power Set	64
5.8.7	The Continuum Hypothesis	65
5.8.8	Martin's Axiom	66
5.8.9	Inaccessible Cardinals and Measurable Cardinals	67
5.8.10	Ordinal Numbers	67
5.8.11	Mathematical Induction	69
5.8.12	Transfinite Induction	69
5.9	A Word About Classes	70
5.9.1	Russell's Paradox	70
5.9.2	The Idea of a Class	70
5.10	Fuzzy Set Theory	71
5.10.1	Introductory Remarks About Fuzzy Sets	71
5.10.2	Fuzzy Sets and Fuzzy Points	71
5.10.3	An Axiomatic Theory of Operations on Fuzzy Sets	72
5.10.4	Triangular Norms and Conorms	74
5.11	The Lambda Calculus	75
5.11.1	Free and Bound Variables in the λ -Calculus	80
5.11.2	Substitution	80
5.11.3	Examples	81
5.12	Sequences	82
5.13	Bags	82

6	Recursive Functions	85
6.1	Introductory Remarks	85
6.1.1	A System for Number Theory	86
6.2	Primitive Recursive Functions	86
6.2.1	Effective Computability	87
6.2.2	Effectively Computable Functions and p.r. Functions	87
6.3	General Recursive Functions	87
6.3.1	Every Primitive Recursive Function Is General Recursive	89
6.3.2	Turing Machines	89
6.3.3	An Example of a Turing Machine	90
6.3.4	Turing Machines and Recursive Functions	90
6.3.5	Defining a Function with a Turing Machine	91
6.3.6	Recursive Sets	91
6.3.7	Recursively Enumerable Sets	92
6.3.8	The Decision Problem	92
6.3.9	Decision Problems with Negative Resolution	93
6.3.10	The μ -Operator	93
7	The Number Systems	95
7.1	The Natural Numbers	95
7.1.1	Introductory Remarks	95
7.1.2	Construction of the Natural Numbers	96
7.1.3	Axiomatic Treatment of the Natural Numbers	97
7.2	The Integers	97
7.2.1	Lack of Closure in the Natural Numbers	97
7.2.2	The Integers as a Set of Equivalence Classes	98
7.2.3	Examples of Integer Arithmetic	98
7.2.4	Arithmetic Properties of the Negative Numbers	98
7.3	The Rational Numbers	98
7.3.1	Lack of Closure in the Integers	98
7.3.2	The Rational Numbers as a Set of Equivalence Classes	99
7.3.3	Examples of Rational Arithmetic	99
7.3.4	Subtraction and Division of Rational Numbers	100
7.4	The Real Numbers	100
7.4.1	Lack of Closure in the Rational Numbers	100
7.4.2	Axiomatic Treatment of the Real Numbers	101
7.5	The Complex Numbers	102
7.5.1	Intuitive View of the Complex Numbers	102
7.5.2	Definition of the Complex Numbers	102

7.5.3	The Distinguished Complex Numbers 1 and i . . .	103
7.5.4	Examples of Complex Arithmetic	103
7.5.5	Algebraic Closure of the Complex Numbers . . .	103
7.6	The Quaternions	103
7.6.1	Algebraic Definition of the Quaternions	103
7.6.2	A Basis for the Quaternions	104
7.7	The Cayley Numbers	104
7.7.1	Algebraic Definition of the Cayley Numbers . . .	104
7.8	Nonstandard Analysis	104
7.8.1	The Need for Nonstandard Numbers	104
7.8.2	Filters and Ultrafilters	105
7.8.3	A Useful Measure	105
7.8.4	An Equivalence Relation	106
7.8.5	An Extension of the Real Number System	106
8	Methods of Mathematical Proof	107
8.1	Axiomatics	107
8.1.1	Undefinables	107
8.1.2	Definitions	108
8.1.3	Axioms	108
8.1.4	Theorems, <i>Modus Ponendo Ponens</i> , and <i>Modus Tollens</i>	108
8.2	Proof by Induction	109
8.2.1	Mathematical Induction	109
8.2.2	Examples of Inductive Proof	109
8.2.3	Complete or Strong Mathematical Induction . .	112
8.3	Proof by Contradiction	113
8.3.1	Examples of Proof by Contradiction	113
8.4	Direct Proof	115
8.4.1	Examples of Direct Proof	115
8.5	Other Methods of Proof	118
8.5.1	Examples of Counting Arguments	118
9	The Axiom of Choice	121
9.1	Enunciation of the Axiom	121
9.2	Examples of the Use of the Axiom of Choice	122
9.2.1	Zorn's Lemma	122
9.2.2	The Hausdorff Maximality Principle	122
9.2.3	The Tukey–Tychanoff Lemma	123
9.2.4	A Maximum Principle for Classes	123
9.3	Consequences of the Axiom of Choice	123
9.4	Paradoxes	125
9.5	The Countable Axiom of Choice	126
9.6	Consistency of the Axiom of Choice	126

9.7 Independence of the Axiom of Choice	126
10 Proof Theory	127
10.1 General Remarks	128
10.2 Cut Elimination	128
10.3 Propositional Resolution	129
10.4 Interpolation	130
10.5 Finite Type	130
10.5.1 Universes	130
10.5.2 Conservative Systems	131
10.6 Beth's Definability Theorem	131
10.6.1 Introductory Remarks	131
10.6.2 The Theorem of Beth	131
11 Category Theory	133
11.1 Introductory Remarks	134
11.2 Metacategories and Categories	134
11.2.1 Metacategories	134
11.2.2 Operations in a Category	135
11.2.3 Commutative Diagrams	136
11.2.4 Arrows Instead of Objects	136
11.2.5 Metacategories and Morphisms	137
11.2.6 Categories	137
11.2.7 Categories and Graphs	137
11.2.8 Elementary Examples of Categories	138
11.2.9 Discrete Examples of Categories	139
11.2.10 Functors	140
11.2.11 Natural Transformations	140
11.2.12 Algebraic Theories	142
12 Complexity Theory	145
12.1 Preliminary Remarks	145
12.2 Polynomial Complexity	146
12.3 Exponential Complexity	146
12.4 Two Tables for Complexity Theory	147
12.4.1 Table Illustrating the Difference Between Poly- nomial and Exponential Complexity	147
12.4.2 Problems That Can Be Solved in One Hour . . .	147
12.4.3 Comparing Polynomial and Exponential Complexity	149
12.5 Problems of Class P	149
12.5.1 Polynomial Complexity	149
12.5.2 Tractable Problems	149

12.5.3	Problems That Can Be Verified in Polynomial Time	149
12.6	Problems of Class NP	150
12.6.1	Nondeterministic Turing Machines	150
12.6.2	NP Contains P	150
12.6.3	The Difference Between NP and P	151
12.6.4	Foundations of NP -Completeness	151
12.6.5	Limits of the Intractability of NP Problems	151
12.7	NP -Completeness	151
12.7.1	Polynomial Equivalence	151
12.7.2	Definition of NP -Completeness	152
12.7.3	Intractable Problems and NP -Complete Problems	152
12.7.4	Structure of the Class NP	152
12.7.5	The Classes Pspace and Log-Space	152
12.8	Cook's Theorem	153
12.8.1	The Satisfiability Problem	153
12.8.2	Enunciation of Cook's Theorem	153
12.9	Examples of NP -Complete Problems	153
12.9.1	Problems from Graph Theory	154
12.9.2	Problems from Network Design	156
12.9.3	Problems from the Theory of Sets and Partitions	156
12.9.4	Storage and Retrieval Problems	157
12.9.5	Sequencing and Scheduling Problems	158
12.9.6	Problems from Mathematical Programming	159
12.9.7	Problems from Algebra and Number Theory	160
12.9.8	Game and Puzzle Problems	161
12.9.9	Problems of Logic	162
12.9.10	Miscellaneous Problems	162
12.10	More on P/NP	163
12.10.1	NPC and NPI	163
12.10.2	Problems in NPI	164
12.10.3	NP -Hard Problems	164
12.11	Descriptive Complexity Theory	164
13	Boolean Algebra	167
13.1	Description of Boolean Algebra	167
13.1.1	A System of Encoding Information	167
13.2	Axioms of Boolean Algebra	168
13.2.1	Boolean Algebra Primitives	168
13.2.2	Axiomatic Theory of Boolean Algebra	169
13.2.3	Boolean Algebra Interpretations	169
13.3	Theorems in Boolean Algebra	170

13.3.1	Properties of Boolean Algebra	170
13.3.2	A Sample Proof	171
13.4	Illustration of the Use of Boolean Logic	171
13.4.1	Boolean Algebra Analysis	172
14	The Word Problem	175
14.1	Introductory Remarks	176
14.2	What Is a Group?	176
14.2.1	First Consequences	176
14.2.2	Subgroups and Generators	176
14.2.3	Homomorphisms	176
14.3	What Is a Free Group?	177
14.3.1	The Definition	177
14.3.2	Words	177
14.4	The Word Problem	177
14.4.1	Extensions of Homomorphisms	177
14.4.2	An Illustrative Example	178
14.5	Relations and Generators	178
14.5.1	Consequences	178
14.5.2	Generators and Relations	179
14.6	Amalgams	179
14.6.1	Free Product with Amalgamation	179
14.6.2	The Free Product	180
14.6.3	Finitely Presented Groups	180
14.7	Description of the Word Problem	181
14.7.1	The Word Problem and Recursion Theory	181
14.7.2	Recursively Presented Groups	181
14.7.3	Solvability of the Word Problem	181
14.7.4	Novikov's Theorem	182
	List of Notation from Logic	183
	Glossary of Terms from Mathematical and	
	Sentential Logic	189
	A Guide to the Literature	219
	Bibliography	231
	Index	237