How To Prove It

HOW TO PROVE IT

A Structured Approach
Third Edition

Daniel J. Velleman
Department of Mathematics and Statistics
Amherst College
Department of Mathematics and Statistics
University of Vermont

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108424189
DOI: 10.1017/9781108539890

First published 1994
Second edition 2006
Third edition 2019

Printed in the United Kingdom by TJ International Ltd, Padstow Cornwall

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data
Names: Velleman, Daniel J., author.
Title: How to prove it : a structured approach / Daniel J. Velleman (Amherst College, Massachusetts).
Description: Third edition. | Cambridge ; New York, NY : Cambridge University Press, [2019] | Includes index.
Identifiers: LCCN 2019013488| ISBN 9781108424189 (hardback : alk. paper) | ISBN 9781108439534 (pbk. : alk. paper)
Subjects: LCSH: Logic, Symbolic and mathematical–Textbooks. | Mathematics–Textbooks. | Proof theory–Textbooks.
Classification: LCC QA9 .V38 2019 | DDC 511.3–dc23
LC record available at https://lccn.loc.gov/2019013488

ISBN 978-1-108-42418-9 Hardback
ISBN 978-1-108-43953-4 Paperback

To Shelley

Contents

Preface to the Third Edition

Students of mathematics and computer science often have trouble the first time they're asked to work seriously with mathematical proofs, because they don't know the "rules of the game." What is expected of you if you are asked to prove something? What distinguishes a correct proof from an incorrect one? This book is intended to help students learn the answers to these questions by spelling out the underlying principles involved in the construction of proofs.

Many students get their first exposure to mathematical proofs in a high school course on geometry. Unfortunately, students in high school geometry are usually taught to think of a proof as a numbered list of statements and reasons, a view of proofs that is too restrictive to be very useful. There is a parallel with computer science here that can be instructive. Early programming languages encouraged a similar restrictive view of computer programs as numbered lists of instructions. Now computer scientists have moved away from such languages and teach programming by using languages that encourage an approach called "structured programming." The discussion of proofs in this book is inspired by the belief that many of the considerations that have led computer scientists to embrace the structured approach to programming apply to proof writing as well. You might say that this book teaches "structured proving."

In structured programming, a computer program is constructed, not by listing instructions one after another, but by combining certain basic structures such as the if-else construct and do-while loop of the Java programming language. These structures are combined, not only by listing them one after another, but also by *nesting* one within another. For example, a program constructed by nesting an if-else construct within a do-while loop would look like this:

```
do
    if [condition]
        [List of instructions goes here.]
    else
        [Alternative list of instructions goes here.]
while [condition]
```

The indenting in this program outline is not absolutely necessary, but it is a convenient method often used in computer science to display the underlying structure of a program.

Mathematical proofs are also constructed by combining certain basic proof structures. For example, a proof of a statement of the form "if P then Q" often uses what might be called the "suppose-until" structure: we *suppose* that P is true *until* we are able to reach the conclusion that Q is true, at which point we retract this supposition and conclude that the statement "if P then Q" is true. Another example is the "for arbitrary x prove" structure: to prove a statement of the form "for all x, $P(x)$," we *declare x to be an arbitrary object* and then *prove* $P(x)$. Once we reach the conclusion that $P(x)$ is true we retract the declaration of x as arbitrary and conclude that the statement "for all x, $P(x)$" is true. Furthermore, to prove more complex statements these structures are often combined, not only by listing one after another, but also by nesting one within another. For example, to prove a statement of the form "for all x, if $P(x)$ then $Q(x)$" we would probably nest a "suppose-until" structure within a "for arbitrary x prove" structure, getting a proof of this form:

```
Let x be arbitrary.
    Suppose P(x) is true.
        [Proof of Q(x) goes here.]
    Thus, if P(x) then Q(x).
Thus, for all x, if P(x) then Q(x).
```

As before, we have used indenting to make the underlying structure of the proof clear.

Of course, mathematicians don't ordinarily write their proofs in this indented form. Our aim in this book is to teach students to write proofs in ordinary paragraphs, just as mathematicians do, and not in the indented form. Nevertheless, our approach is based on the belief that if students are to succeed at writing such proofs, they must understand the underlying structure that proofs have. They must learn, for example, that sentences like "Let x be arbitrary" and "Suppose P" are not isolated steps in proofs, but are used to introduce the "for arbitrary x prove" and "suppose-until" proof structures. It is

not uncommon for beginning students to use these sentences inappropriately in other ways. Such mistakes are analogous to the programming error of using a "do" with no matching "while."

Note that in our examples, the choice of proof structure is guided by the logical form of the statement being proven. For this reason, the book begins with elementary logic to familiarize students with the various forms that mathematical statements take. Chapter 1 discusses logical connectives, and quantifiers are introduced in Chapter 2. These chapters also present the basics of set theory, because it is an important subject that is used in the rest of the book (and throughout mathematics), and also because it serves to illustrate many of the points of logic discussed in these chapters.

Chapter 3 covers structured proving techniques in a systematic way, running through the various forms that mathematical statements can take and discussing the proof structures appropriate for each form. The examples of proofs in this chapter are for the most part chosen, not for their mathematical content, but for the proof structures they illustrate. This is especially true early in the chapter, when only a few proof techniques have been discussed, and as a result many of the proofs in this part of the chapter are rather trivial. As the chapter progresses, the proofs get more sophisticated and more interesting, mathematically.

Chapters 4 and 5, on relations and functions, serve two purposes. First, they provide subject matter on which students can practice the proof-writing techniques from Chapter 3. And second, they introduce students to some fundamental concepts used in all branches of mathematics.

Chapter 6 is devoted to a method of proof that is very important in both mathematics and computer science: mathematical induction. The presentation builds on the techniques from Chapter 3, which students should have mastered by this point in the book.

After completing Chapter 6, students should be ready to tackle more substantial mathematical topics. Two such topics are presented in Chapters 7 and 8. Chapter 7, new in this third edition, gives an introduction to number theory, and Chapter 8 discusses infinite cardinalities. These chapters give students more practice with mathematical proofs, and they also provide a glimpse of what more advanced mathematics is like.

Every section of every chapter ends with a list of exercises. Some exercises are marked with an asterisk; solutions or hints for these exercises are given in the appendix. Exercises marked with the symbol $^{\text{PD}}$ can be done using Proof Designer software, which is available free on the internet.

The biggest changes in this third edition are the addition of a new chapter on number theory and also more than 150 additional exercises. The section

on reflexive, symmetric, and transitive closures of relations has been deleted from Chapter 4 (although these topics are now introduced in some exercises in Section 4.4); it has been replaced with a new section in Chapter 5 on closures of sets under functions. There are also numerous small changes throughout the text.

I would like to thank all those who sent me comments about earlier editions of this book. In particular, John Corcoran and Raymond Boute made several helpful suggestions. I am also grateful for advice from Jonathan Sands and several anonymous reviewers.