高阶逻辑辅助证明系统

A PROOF ASSISTANT FOR HIGHER-ORDER LOGIC

[德]托比亚斯·尼普科夫 Tobias Nipkow
[英]劳伦斯·鲍尔森 Lawrence C. Paulson
[德]玛尔库斯·温泽尔 Markus Wenzel 著
陈光喜 刘卓军 译

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

高阶逻辑辅助证明系统

[德]托比亚斯·尼普科夫 Tobias Nipkow
[英]劳伦斯·鲍尔森 Lawrence C. Paulson
[德]玛尔库斯·温泽尔 Markus Wenzel 著
陈光喜 刘卓军 译

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

高阶逻辑辅助证明系统/(德)尼普科夫(Nipkow,T.),(英)鲍尔森(Paulson,L.C.),(德)温泽尔(Wenzel,M.)著;陈光喜,刘卓军译.—北京:北京理工大学出版社,2013.5

ISBN 978-7-5640-7763-1

Ⅰ.①高…　Ⅱ.①尼…②鲍…③温…④陈…⑤刘…　Ⅲ.①计算机辅助技术　Ⅳ.①TP391.7

中国版本图书馆 CIP 数据核字(2013)第 109015 号

版权登记号:图字:01-2013-3017

出版发行 /北京理工大学出版社
社　　址 /北京市海淀区中关村南大街 5 号
邮　　编 /100081
电　　话 /(010)68914775(办公室)　68944990(批销中心)　68911084(读者服务部)
网　　址 /http://www.bitpress.com.cn
经　　销 /全国各地新华书店
印　　刷 /北京通州皇家印刷厂
开　　本 /850 毫米×1168 毫米　1/32
印　　张 /8.5
字　　数 /204 千字　　责任编辑 /陈莉华
版　　次 /2013 年 5 月第 1 版　　文案编辑 /张　盟
　　2013 年 5 月第 1 次印刷　　责任校对 /杨　露
定　　价 /45.00 元　　责任印制 /王美丽

中文版序

19世纪的后半期，数学家们开始对自己的学科，尤其是对证明到底是什么感到了疑惑。这导致了现代逻辑的诞生，进而使得数学的牢固基础得以建立。但数学证明的实践却几乎没有受到影响：详细的逻辑证明构造起来太长并且太过复杂。进入20世纪的后半程之后，计算机科学家接受了这个挑战，提出建立被称为证明助手的系统，借助这样的系统你可以以交互的方式构造证明而由系统去检查逻辑细节。在21世纪的今天，证明助手已经被用于验证复杂软件，诸如编译器和操作系统内核的正确性，以及证明相当深刻的数学定理。无论是在学术研究领域还是在工业界，证明助手开始改变着关键软件的开发方式。为了使21世纪成为应用逻辑的黄金时期，证明助手领域的工作正在提供着助力。

本书介绍了证明助手领域的一项先驱性工作Isabelle/HOL。我们在十多年前写了这本书，目前它已经成为被广泛引用的经典文献。在过去的十年里，证明助手这一领域发生了迅速变化，Isabelle/HOL也是如此。本书的内容也随着研究的深入而不断更新和发展。例如，结构化的证明风格已经被引入，现在可以基于Isabelle/HOL的文件生成证明代码。我们鼓励读者仔细研究Isabelle网站isabelle.in.tum.de提供的英语版手册，以便获取Isabell近期发展的进一步的信息。在这个网站还可以发现很多练习题目和需要思考的问题。这本书是关于Isabelle/HOL的综合入门文献，包含许多例子来解释基本和高级的特征，其中的一些是非常本质性的内容。我们非常高兴这本书有了中文版本，向在相关工作中作出贡献的陈光喜博士和刘卓军博士表示衷心的感

谢。我们希望这本书会让更多的学生、教师和研究人员认识和了解证明助手这一精彩的领域，并为这一领域的发展贡献出他们的智慧。

2012 年 12 月

Tobias Nipkow，德国慕尼黑技术大学
Lawrence C. Paulson，英国剑桥大学

Preface for Chinese Edition

In the second half of the 19th century, mathematicians started to wonder about the foundations of their subject and in particular about what a proof is. This was the birth of modern logic, which gave mathematics a firm foundation. But the practice of mathematical proof was hardly affected: detailed logical proofs were much too long and complicated to construct. In the second half of the 20th century, computer scientists took up this challenge and designed what are now known as Proof Assistants systems that allow you to construct proofs in an interactive fashion while the system checks the logical details. Now, in the beginning of the 21st century, Proof Assistants have been used to verify the correctness of complicated software like compilers and operating system kernels as well as of extremely deep mathematical theorems. Proof Assistants are beginning to transform the way in which critical software is built, both in research and in industry. The work of the Proof Assistant community is helping to make the 21st century the golden age of applied logic.

This book introduces Isabelle/HOL, one of the world's leading Proof Assistants. We wrote the book more than 10 years ago and it has become a widely-cited classic. In that 10 years, the field has evolved rapidly, as has Isabelle/HOL. For example, an alternative style of structured proofs has been introduced and it is now possible to generate code from Isabelle/HOL files. The reader is encouraged to explore the Isabelle web site isabelle. in. tum. de for further

English language manuals explaining more recent developments. Many exercises and problems can also be found there. This book remains a comprehensive introduction to Isabelle/HOL, covering basic and advanced features with many examples, some of which are very substantial. We are happy that this book is finally available in Chinese. Our sincere thanks go to Dr. Guangxi CHEN and Dr. Zhuojun LIU who contributed to this work. We hope that it will allow many more students, teachers and researchers to learn about the wonderful world of Proof Assistants and to contribute to its exciting future themselves.

December 2012

Tobias Nipkow, Technische Universitat Munchen (TUM)

Lawrence C. Paulson, Universityof Cambridge, UK

前　言

本书是在高阶逻辑中使用 Isabelle 辅助证明系统进行交互式证明的导论，适用于 Isabelle 系统的潜在使用者，自成体系，分为三部分：

——第一部分是基本技巧：介绍在高阶逻辑中如何进行函数式程序建模，提供了表(list)和自然数的简单证明实例。大多数证明只要两步完成：对所选变量进行归纳以及使用自动策略(auto)。当然，这些粗浅的例子仍然涵盖了嵌套递归和交叉递归等技术。

——第二部分是逻辑与集合：介绍大量可供选择使用的低级证明策略。本部分描述了 Isabelle/HOL 如何处理集合、函数、关系以及如何实现递归定义集合，包括模型检验理论和经典教科书中关于形式语言的案例。

——第三部分是高级话题：包括实数、记录、重载技术等主题。本部分也讨论了归纳法和递归方法的高级技巧，还专门给出一章来介绍安全协议的形式化验证。

本书的排版是使用 Wenzel 的理论文件展示工具来完成的，类似于 Latex 源文件编写方式。本书几乎完全采用这种方式完成编排，第一部分的最后一章向读者介绍了如何使用类似的方式来产生自己的格式文档。

Isabelle 主页[①]给出了各种下载链接和相关信息。大多数 Isabelle 会话都可在 David Aspinall 开发的 Proof General[②] 用户

① http://Isabelle.in.tum.de/

② http://Proof General.inf.ed.ac.uk/

界面上运行，甚至可以结合 XEmacs 的 X-Symbol 包[①]一起使用。本书很少介绍 Proof General 系统，读者可以查到它本身的使用文档。要运行 Isabelle，读者需要标准的 ML 编辑器，建议使用 Poly/ML[②]，它是免费的，而且性能优良。另一个全支持编辑器是 New Jersey 的 Standard ML[③]。

我们要感谢 Munich 的 Isabelle 研究组的同仁经常性的讨论和有价值的反馈意见。他们是：斯蒂凡·伯格霍夫、奥拉夫·穆勒……。也要感谢斯蒂芬·梅兹仔细阅读草稿并提出了宝贵意见。斯蒂法诺·比塞塔热利等也提供了很好的建议。

相关研究得到了多项基金的支持，包括 DFG 资助的 NI 491/2，NI 491/3，NI 491/，NI 491/6；BMBF 项目的 Verisoft；EPSRC 资助的 GR/K57381，GR/K77051，GR/M75440，GR/R01156/01，GR/S57198/01 以及 ESPRIT 工作组资助的 21900、IST－1999－29001 等。

① http://X－Symbol. sourceforge. net

② http://www. polyml. org/

③ http://www. smlnj. org/index. html

目　录

第一部分　基本技巧

第二部分 逻辑与集合

第三部分 高级材料

第一部分　基本技巧