国家自然科学基金研究专著
NATIONAL NATURAL SCIENCE FOUNDATION OF CHINA

信息科学系列

数字硬件的形式化验证

韩俊刚 杜慧敏

北京大学出版社

国家自然科学基金研究专著
NATIONAL NATURAL SCIENCE FOUNDATION OF CHINA

数字硬件的形式化验证

韩俊刚 杜慧敏

北京大学出版社
·北京·

图书在版编目(CIP)数据

数字硬件的形式化验证/韩俊刚,杜慧敏著. —北京:北京大学出版社,2001.12

ISBN 7-301-05332-0

Ⅰ.数… Ⅱ.①韩… ②杜… Ⅲ.数字系统-系统设计-形式化-验证 Ⅳ.TP271

中国版本图书馆 CIP 数据核字(2001)第 082714 号

书　　名:数字硬件的形式化验证

著作责任者:韩俊刚　杜慧敏

责任编辑:顾卫宇

标准书号:ISBN 7-301-05332-0/TP·0632

出 版 者:北京大学出版社

地　　址:北京市海淀区中关村北京大学校内　100871

网　　址:http://cbs.pku.edu.cn

电　　话:出版部 62752015　发行部 62754140　理科编辑部 62752021

电子信箱:zpup@pup.pku.edu.cn

排 版 者:北京高新特激光照排中心　62637627

印 刷 者:北京大学印刷厂

发 行 者:北京大学出版社

经 销 者:新华书店

850×1168　32 开本　8.75 印张　231 千字

2001 年 12 月第 1 版　2001 年 12 月第 1 次印刷

定　　价:18.00 元

序　言

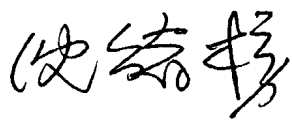
集成电路的主流制造工艺正在向深亚微米发展.使用传统的基于模拟的方法对含有几百万门的电路和系统设计进行验证,已经不能满足设计的需要.因此对于这样复杂的电路和系统,人们正在寻求其他的设计验证技术作为补充,比如硬件仿真和形式化验证就是适应这个要求而产生的新技术.最近,世界上著名的 EDA 公司如 Cadence 和 Synopsys 等都在研制并相继推出形式化验证工具,特别是等价性检验和模型检验工具,并把这些工具集成到他们的 EDA 设计环境中.

随着系统芯片(SOC)设计日趋复杂化,设计验证工作越发繁重.据统计在很多复杂的集成电路的设计中,验证过程消耗了整个设计周期的三分之二,设计过程所需要专门的验证工程师的人数一般是 RTL 设计工程师人数的二倍.在设计完成时,测试向量编码构成全部设计编码的 80%.可见功能验证已经成为 SOC 设计的瓶颈.

本书作者多年来研究形式化方法在硬件设计和验证中的应用,并得到了国家自然科学基金的多次支持,取得了可喜的成果.本书作者结合自己的成果介绍硬件形式化验证的原理和技术,对于我国集成电路设计者学习和应用形式化验证方法是很有价值的.

我国正在大力发展集成电路产业.集成电路是电子工业的粮食,是信息产业的基础.集成电路对于提高电子产品的性能、降低电子产品的价格起着关键的作用.要为我国正在建立和已经建立的集成电路生产线提供源源不断的设计,需要广大集成电路设计

人员掌握现代的设计和验证方法.因此,我相信本书的出版将为我国的集成电路设计验证方法的研究和应用作出贡献.



2001 年 9 月

前　言

当今微电子技术的发展，使得含有数百万门的集成电路已经能够大批量地生产出来，真正的系统芯片(system on chip)正在成为现实. 但是如何正确地设计这些复杂的超大规模集成电路的问题还没有解决. 可以说集成电路制造的能力超过了集成电路的设计能力. 为了充分发挥投资惊人的集成电路生产线的生产能力，需要更多的设计者及时地提供大量复杂的设计. 另外，计算机技术和通讯技术的高速发展，使得数字系统渗透到整个社会的各个领域，特别是对于安全性要求极高的很多关键的场合也大量地采用了嵌入式系统；同时各种数字硬件的设计变得十分复杂，用传统的设计方法已经难以应付. 这些都是对电路和系统设计者的严峻的挑战. 设计大规模的复杂的数字系统中的关键问题之一是如何检查设计的正确性，即设计验证. 但是，设计验证的复杂度随着芯片的规模呈指数增加. 传统的验证手段是模拟(simulation)、测试(testing)和仿真(emulation)技术，但是对于大型的系统，模拟和测试都不可能是完全的，只能针对某些典型的情况或者随机地进行，这就难以完全排除所有的设计错误. 由于集成电路的工艺的复杂性，它的试制费用相当昂贵；又由于电子产品市场的剧烈竞争，产品上市的时间极为重要. 设计中遗留的一点微小的错误将可能造成巨大的经济损失或者引起人员伤亡等灾难性的后果. 据统计，设计验证的时间占整个设计周期的 50%～80%. 因此设计的正确性验证成为设计的瓶颈，被称为“验证危机”.

在软件设计中也具有类似的问题，即程序的正确性验证问题. 在 60 年代末兴起的软件验证技术就反映了计算机科学家和数学家为解决“软件危机”，即软件设计正确性问题所做的努力. 他们利

用数学理论和方法严格地证明程序的正确性.这些努力在程序设计方法学方面做出了很大的贡献.然而一般认为软件验证技术在工业界的应用基本上是不成功的.80年代初,人们把类似的方法用来验证硬件,产生了硬件的形式化验证技术.目前普遍认为,硬件验证技术在工业界的应用前景是十分乐观的.现在可以说,硬件形式化验证技术的推广应用正在迅速展开.出现这种情况的原因之一是软件和硬件在复杂度方面具有很大的差别.即使最复杂的硬件,比典型的软件的复杂程度也要小得多.这就使得对于硬件可以有效地应用基于状态空间法的工具如模型检验程序.另一个重要的原因是软件验证和硬件验证在本质上具有不同的特点.软件验证经常需要用户利用自己的知识和经验相当深入地指导验证过程,但是硬件验证系统可以有效地利用自动状态穷举、语言包含和符号重写等方法进行自动验证.由于硬件具有比软件更好的模块性,经常可以把一个大规模的验证问题分解为若干孤立的规模较小的问题,然后用自动化工具解决.事实上,硬件验证的理论和方法的研究和应用在近十几年来发展很快.特别是最近几年,某些方面取得了突破性进展.前几年被认为没有前途的硬件设计的形式化验证技术得到了工业界的普遍认可,特别是模型检验技术,已经引起了EDA产业的轰动和商业界的投资热潮.据统计,近几年在全世界的主要EDA公司都相继研制和推出了形式化验证的软件.人们预计这项技术将在电子设计领域得到更加广泛的应用.但是在国内,这种情况尚未引起广泛重视,甚至很多人对于形式化验证感到陌生.

本书将要介绍的就是数字硬件的形式化验证技术.其目的是使国内的电路设计者了解这个新领域,适应这一新技术的迅速的发展,特别是为高等学校的相关专业的教师、研究生和高年级学生学习这一新技术提供参考,为在工业界推广应用形式化验证技术在教育方面准备条件.

形式化验证技术的数学工具包括数理逻辑、集合论、图论和代

数理论. 对于这些知识的深度的要求基本上没有超出大学离散数学课程. 因此相近专业的大学高年级学生应该能够顺利地阅读本书的大部分内容. 当然,读者应当具有数字电路设计和计算机科学理论的基本知识.

本书的作者在国家自然科学基金的多次资助下近十年来一直跟踪和研究硬件设计的形式化验证技术;结合自己的研究工作,对国外的主要研究工作也做了深入的考查和广泛的实验. 本书是对国内外硬件验证技术成果的总结和介绍,也总结了作者的部分研究工作. 但是考虑到本书的社会效果,并不把重点放在最新的研究课题上,而是把介绍较为成熟的新技术、新方法作为主要目标. 这样可以使较为广泛的读者能够阅读本书,并把这些新技术应用到实际的电路设计工作中去. 当然,作为一本专著,也要介绍该领域的最新研究方向和成果. 这样既能引起广大硬件设计者对于这一新技术的兴趣,又会对将要进入本领域进行研究的读者有所帮助.

硬件设计形式化验证的主要技术可以分为两个方面,即基于定理证明技术的验证和基于模型检验技术的验证. 这两种技术目前都开始走向成熟和实用化. 为了便于读者通过实践学习这些技术,我们用剑桥大学的高阶逻辑系统的最新版本 HOL98 作为实际练习的环境来学习利用定理证明技术验证硬件设计的方法;同时我们利用加利福尼亚大学伯克利分校的 VIS 系统作为学习模型检验技术的实验环境. 这两个系统都可以在微机的 Linux 操作系统上运行. 这也有利于在高校的计算机科学技术、电子信息工程等相关专业为研究生开设“形式化方法”、“机器定理证明”等课程时参考本书的内容.

本书的第一章对形式化方法做一般的介绍:回顾近年来该领域的发展情况,展望将来的可能的发展趋势,讨论形式化方法的特点和局限性. 第二章介绍数字设计验证的基本概念和一般方法,包括规范和实现、硬件描述和验证、形式化系统和定理证明系统等. 第三章介绍剑桥大学的高阶逻辑系统 HOL98 及其在硬件验证中

的应用. 以加法器和微处理器的验证为例说明如何用 HOL 系统进行硬件验证. 第四章介绍模型检验技术，包括分支时态逻辑、二叉判定图、符号模型检验等. 第五章介绍美国加州大学伯克利分校的 VIS 系统和我们利用 VIS 系统验证微处理器设计的方法和经验. 第六章介绍自动机理论的新发展和基于自动机理论的形式化验证方法，这也是近年来在形式化验证方面研究的热点.

本书的第一、二、三章由韩俊刚编写，第四、五、六章由杜慧敏编写. 由于水平限制，书中的谬误和疏漏之处在所难免，希望读者不吝赐教.

多年来支持和帮助我们的有中国科学院软件所的唐稚松院士、英国 Leeds 大学的 G. Birtwistle 教授、英国剑桥大学的 M. J. C. Gorden 教授、中国科学院计算技术研究所的林宗楷教授、北京理工大学的刘明业教授、清华大学的薛宏熙和边计年教授. 与作者共同工作过并为本书做出贡献的有朱宾博士、殷勇博士、王岩冰博士、霍红卫博士等. 在此一并致谢.

作　者

2000 年 10 月于西安

目　录

第一章　形式化方法

本书的主要内容是讲述数字硬件设计领域的形式化验证技术，它是形式化方法在硬件设计中的应用，因此本章先介绍一般的形式化方法. 形式化方法是计算机科学的一个较为广泛的应用研究领域. 对它有了一般的了解，读者就能站在一定的高度上理解以后各章的内容.

1.1　什么是形式化方法

形式化方法对不同的应用领域可能具有不同的含义. 因而有人说“形式化方法对不同的人是不同的东西”. 形式化方法的具体应用领域极为广泛，如铁路信号系统、航空航天系统、核电站控制系统、通讯系统、医疗保健系统、集成电路、测量仪表等等. 要弄清什么是形式化方法，首先要弄清它的研究对象、研究目的、研究方法和特点. 目前，形式化方法的主要研究对象是计算机系统的设计和验证. 这里的计算机系统可以是硬件系统、软件系统、嵌入式系统(embedded system)、分布式系统(distributed system)、反应式系统(reactive system)、实时系统(real-time system)、混合系统(hybrid system)，等等. 形式化方法的最主要的目的是帮助工程师构造正确可靠的计算机系统. 形式化方法的最基本的特点是利用数学的概念、方法和工具来解决设计的正确性问题. 作为形式化方法的主要数学基础包括各种逻辑学、集合论、代数理论、图论等.

一般说来，形式化方法就是用具有形式语义的记号和工具明确地表述所要设计的计算机系统的设计要求，即给出系统规范(specification)，并根据系统规范利用上述记号和工具对系统具有

的性质和最终实现的正确性进行严格的证明.

形式化方法这个术语本身的含义并不确切."形式"可能来源于形式逻辑和形式语言.对于软件系统设计,目前大多数应用中主要用形式化方法来明确地表达软件的需求和规范."形式化方法"中的"方法"则更多地含有"形式化系统"的意义.实际上一种形式化方法是由某种形式化的语言及其相关的工具(例如编译器、查错程序、验证程序等)构成的一套形式化系统.

形式化方法并不是新概念.实际上,在现代各个工程领域的人们都在自觉或不自觉地在计算、模拟、测试中应用数学方法,甚至进行公式推导和证明.例如人们用布尔代数来设计继电器开关电路和数字逻辑电路;在程序设计中大量使用逻辑、集合、图论和代数来建立数据结构、构造算法和验证程序.可以说,有了数学的应用,就有了形式化方法.但是一般认为形式化方法是从60年代末程序验证的研究开始.当时由于"软件危机",人们企图用数学方法证明程序的正确性而发展了各种程序验证方法.比较著名的有Floyd、Hoare和Manna等人的方法.但是利用这些技术所验证的程序的规模受到限制,难以实用化.到80年代末,许多程序验证研究人员转向硬件验证.人们认为硬件比软件相对地简单,可望用已有的方法和工具很快取得成果.实际上,在系统设计的较高层次上,软硬件的设计没有差别.但是由于作为硬件设计规范的硬件描述语言(如VHDL和Verilog)已经广泛被采用,所以硬件的形式化方法集中在设计验证方面.而且多数硬件验证的研究工作利用了原来程序验证的成果,并后来居上地取得了突破性的进展.而软件方面的形式化方法则仍集中应用在软件规范的形式化描述,即严格地表达用户需求,形成明确的、一致的、有时是可运行的系统规范,从而在设计的早期就发现可能存在的不一致性和不完全性,有的也支持在后来的逐步求精的过程中的验证和检查.

形式化方法与计算机科学和数学的关系是什么?这是值得讨论和思考的.目前存在不同的说法.有人认为形式化方法可以作为

纯数学的一个分支，也可以作为软件工程的一个分支. 有人认为“形式化方法是用于计算机系统工程的应用数学”. E. M. Clarke 认为形式化方法是一个与计算机科学的各个领域几乎都交叉的研究领域. 英国计算机科学家 R. Milner 认为计算机科学(计算的理论)就是构造模型(概念)并对它们进行形式化处理的(科学). 但是他认为如果把形式化方法与计算机科学等同起来而忘记了理论化就低估了计算机科学.

我们认为形式化方法就是面向计算机系统设计实践的应用计算机科学，它也包括一些相关的理论研究，这些理论研究是以设计和验证计算机系统为直接目标的. 设计和验证计算机系统的实践给形式化方法提出问题，这些问题的研究又丰富和发展了理论计算机科学. 计算机科学同其他科学一样都需要采用适当的数学为基础并与之相结合共同发展. 例如可计算性和自动机理论、算法和复杂度理论、语义学和形式语言等与数理逻辑、集合论等都是密不可分的. 目前各种时态逻辑的理论和实时自动机的理论就是在研究系统的定时问题的描述和验证中，在实时系统和实时程序的设计和验证中产生的. 而混合自动机则是实时自动机的自然的推广. 实际上，计算机科学的发展总是伴随着数学的应用而与数学互相渗透并共同发展的.

形式化方法的研究领域包括具体的设计和验证技术到抽象的一般性理论的研究. 其研究对象和方法的抽象层次、研究中采用的数学工具和研究对象的覆盖范围都极为广泛，而且还在不断扩大. 也许正是由于这个原因使得在这个“广谱”的领域中，人们处于不同的层次、使用不同的工具、研究不同的对象，因而经常出现对形式化方法的不同观点. 比如，有的人说形式化方法的研究应走在实践的前面，而有的人说形式化方法的研究应从实践出发；有的人认为形式化方法的研究取得了巨大成就，而有的人说形式化方法的研究没有多大价值；有的人推崇“完全的形式化”，而有的人说“完全的形式化是不可能的”. 热心形式化方法的人们总是对其成熟程

度估计过高，而来自“第一线”的实践家经常说它“最多是一个不重要的壁龛(niche)技术”.

计算机科学尚处于幼年阶段，甚至是“刚刚开始的阶段”，以至于有人说“计算机科学还不是科学”. 形式化方法作为计算机科学与实际应用的桥梁，它的应用对象是在飞速发展、不断变化的，它的应用领域又是在不断开拓、不断扩展的. 这些变化和扩展常常出乎人们意料. 因此我们不应当指责它本身没有能够取得预期的成果，也不能指望它的理论在短期内全面地、成功地应用于整个计算机系统设计领域. 尽管它已有三十年的历史，但仍然是年轻而不成熟的.

对于本书将要介绍的数字硬件的设计和验证，形式化方法也许是最有成效的领域，以后将会看到，近几年，形式化方法首先在数字硬件验证方面取得了突破性进展.

1.2 形式化方法的意义和局限性

1.2.1 形式化方法的意义

在一本著名的“软件工程”教科书(第三版)中，作者对形式化方法是如此评价的：“计算机科学领域一些热心形式化方法研究的人们不了解实际的软件工程而鼓吹采用形式化方法进行软件开发，但实用的软件工程非常不同于他们的解决办法.”

这里的实质问题是：形式化方法是否是从学术界“杜撰”出来的不切实际的方法？它是否能作为解决设计正确的计算机系统的问题的有效途径？

著名计算机科学家，程序逻辑的创始人 C. A. R. Hoare 回顾了近些年来的软件工程的实践后，认为软件工程面临的实际情况比我们在十年前预计的要好得多. 他承认“虽然形式化方法的研究有了很大的进步并对设计实践产生了重要的、日益强大的冲击，但