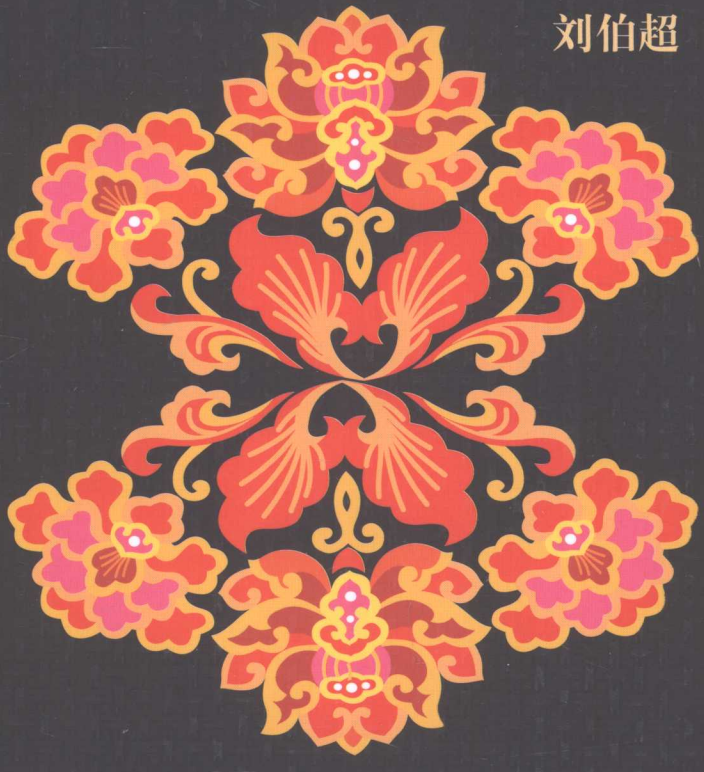
世界著名计算机教材精选

软件工程 卷3

领域、需求与软件设计

Dines Bjørner 著
刘伯超 向剑文 等译



SOFTWARE ENGINEERING 3

Domains, Requirements, and Software Design

清华大学出版社

SOFTWARE ENGINEERING 3 Domains, Requirements, and Software Design

软件工程 卷3 领域、需求与软件设计

《软件工程卷1～3》是冯诺依曼奖章获得者、世界著名的计算机科学家Dines Bjørner教授的最新著作。这套丛书为读者理解软件和软件开发过程提供了一个“全新的视角”。这三卷书首次系统地论述了如何用形式方法来指导领域工程、需求工程和软件设计，即软件工程的三个相互关联并重叠的组成部分，或称之为软件工程的“三部曲”。在软件开发的各个阶段，如果都能够采用这种形式化的开发模式，将能够在极大程度上保证软件开发的正确性和有效性。

这套丛书可以被视为软件工程史上里程碑式的著作。作者通过长达30年的程序设计方法论的研究与实践，加上长达25年不断完善的课程讲义汇编成这一套前后连贯、内容一致以及相对完整的软件工程著作。这套丛书的一个显著特点就是在这三卷书中，所有的原理、技术和工具都是通过大量的案例分析来进行阐述，并覆盖了所有主要的软件开发时期、阶段和步骤；同时，这些原理、技术和工具是能够应用在大型工业和商业软件的开发项目中去的。

这套丛书不但可以作为高校计算机专业学生、教师以及研究人员的教材和必备参考书，而且在工业和计算机产业界也具有极大的实用价值。

《软件工程卷1：抽象与建模》介绍了抽象与建模的基本原理和技术。首先，本卷给出了离散数学的基本介绍，包括数、集合、笛卡尔、类型、函数、λ-演算、代数和数理逻辑，然后讲授基本的面向属性与面向模型的规约的基本原理和技术。一些其他的规约语言，比如B、VDM-SL和Z都具有面向模型的概念，本卷则通过RAISE规约语言RSL来讲解这个概念。本卷还介绍了有关应用式（函数式）、命令式和并发式（并行式）规约程序设计的基本原则。最后，本卷给出了一个全面的软件工程术语表以及大量的索引和参考文献。

《软件工程卷2：系统与语言规约》介绍了描述系统与语言的规约的基本原理和技术。首先，本卷讲授一些高级的原理和技术：分层与组合、指称与计算以及构型；环境与状态的抽象与建模，然后讲授符号学建模的基本原理和技术：语用、语义以及系统和语言的句法。其中重要的一部分介绍了对空间和简单时态现象进行建模的基本原理和技术。本卷的主要章节用于介绍一些专门的主题，比如模块（包括UML的类图）、Petri网、活动序列图、状态图和时态逻辑（包括时段演算）。最后，本卷介绍了开发函数式，命令式以及并行程序设计语言的可靠和有效的解释器和编译器的基本原理和技术。本卷适合于作为高年级本科生和研究生，以及研究程序设计方法学的学者的教材或参考书。

《软件工程卷3：领域、需求与软件设计》介绍了整体软件开发的基本原理和技巧：从领域描述，经过需求分析，直到软件设计。本卷倡导一种全新的软件工程开发模式：在需求被形式化之前，人们必须理解应用领域，因此本卷首先介绍领域描述的原理和技术，然后介绍从领域模型导出需求规则的原理和技术，最后介绍细化需求到软件设计的原理和技术：体系结构和组件设计。

ISBN 978-7-302-20892-1

定价：79.00元

世界著名计算机教材精选

Software Engineering 3

Domains, Requirements, and Software Design

软件工程卷 3

领域、需求与软件设计

Dines Bjørner 著

刘伯超 向剑文 等译

清华大学出版社

北 京

北京市版权局著作权合同登记号　图字 01-2007-0329 号

图书在版编目(CIP)数据

软件工程卷 3：领域、需求与软件设计/（德）比约尼尔（Bjørner, D.）著；刘伯超等译. —北京：清华大学出版社，2010.1
（世界著名计算机教材精选）
书名原文：Software Engineering 3: Domains, Requirements, and Software Design
ISBN 978-7-302-20892-1

Ⅰ. 软…　Ⅱ. ①比 …　②刘 …　Ⅲ. 软件工程－教材　Ⅳ. TP311.5

中国版本图书馆 CIP 数据核字（2009）第 159919 号

责任编辑：龙啟铭
责任校对：徐俊伟
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：39　**字　数**：972 千字
版　　次：2010 年 1 月第 1 版　　**印　　次**：2010 年 1 月第1 次印刷
印　　数：1～3000
定　　价：79.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　产品编号：023238-01

Nikolaj、Marianne、Katrine 与 Jakob

我眼中的希望之光

没有理论
没有证明
可能有大胆的推测
将会有糟糕的证伪

Imre Lakatos 与 Sir Karl Popper 的自由解释 [204, 273, 274, 276]

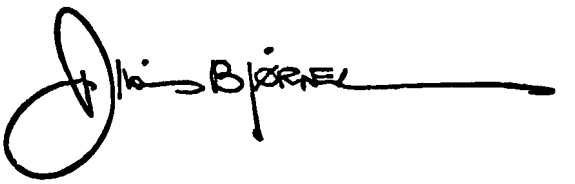
原著作者为中文版所作的序

在妻子和我的家中，有许多纪念品。它们来自于我们对中国超过 50 次的访问以及我在中国澳门担任由联合国和中国共同创建的联合国大学国际软件技术研究院的首任院长为期 5 年时间的纪念品：20 多件从 18 世纪 60 年代到 1910 年的清代花瓶；三套成对的中国灯挂椅、马掌椅、低背椅。这些和一张非常棒的一米宽、两米长的黄花梨四柱卧床（原名如此！）装饰了我们的大客厅—— 伴上精雕细刻的中国屏风和五彩斑斓的中国玻璃窗，它们时时刻刻都让我们想起一个伟大的文化和卓越的工艺。14 年前我们的女儿和一位年轻的中国人结婚了，他们和我们的两个外孙女促使我们更加热爱中国和中国人民。

所以在 2006 年 8 月当刘伯超博士和他的同事们询问是否可以翻译我的三卷著作的时候，我自然会欣然接受了。我的著作，它代表着 25 年的劳动：思考、教学和写作。我非常高兴中国的优秀青年现在能够学习我的著作了。

要想真正成为计算科学和软件工程的专家，你必须要喜欢阅读和写作。现在你有机会来阅读了。阅读的同时，把你的所学应用到书写漂亮、抽象的规约中来。

我祝你愉快。我真心希望我的读者将享受计算科学、程序设计和软件工程的实践，就像我所享受到的并仍在享受它一样。



Dines Bjørner

Holte，丹麦，2007 年 8 月

译者序

本书是世界著名的计算机科学家 Dines Bjørner 教授对其所从事的软件工程研究的总结。

这几卷书主要讲述了如何使用形式方法指导软件工程的开发，特别是作者独创性地提出了领域工程这一全新的研究领域并在第 3 卷中予以系统的论述。作者结合 RAISE（工业软件开发的严格方法）规约语言，详细阐释了在软件的领域分析、需求分析、软件设计和开发的各个阶段，如何采用形式方法来指导软件开发模式，来保证软件开发的可靠性和正确性。

在翻译的过程中，译者得到了 Dines Bjørner 教授的大力支持。他非常关心中国学者在软件工程这一领域的研究，热心推动我们将他的三卷著作介绍给中国读者。

向剑文翻译了前言和第 1 章，刘伯超翻译了第 2~16、19~21、26~32 章以及附录，都玉水翻译了第 17~18、22~25 章。参加翻译和校对工作的还有田璟、王明华、袁春阳、李智伟、周琼琼、楚国华、齐亮、司慧勇、陈永然、李佳。限于译者水平，译文中难免会出现一些错误和不妥之处，敬请读者和专家予以批评指正。

前言

概述

本卷是有关软件工程的工程原则与技术的三卷教材中的第 3 卷。通过这三卷书我们宣称我们展示了形式技术（也被称之为形式方法）是如何可以在大规模开发项目中得以最大限度地使用。我们进一步提出：我们现在可以有理由宣称不再有任何借口不在开发的所有时期、阶段与步骤中使用形式技术。通常给出这样的借口是由于缺少在超大规模软件开发中使用形式技术的全面指南。这里就是十分详细地告诉你如何来做其中绝大多数事情的一套丛书！

当然，不是所有开发刻面现今都被详细说明到我们本希望可使用形式技术的层次。但是抑制使用现有的形式技术——在我们或许不是那么谦逊的看法来看——完全是犯罪！正如这几卷以及许多现有的优秀的专著所揭示的那样：不使用这些技术的傲慢可以简单地归结为犯罪性的忽略。

一些所谓的软件工程实践者“坚持”缺乏管理指南。对于他们，我要说：一旦你已经理解这几卷的原则与技术，并且如果你另外具有一些管理经验和判断力，那么其余的自然就得到了。你和我可以“填写”这些管理原则与技术。

卷 1 的附录 B 包含一个详尽的术语表，并且卷 2 的附录 A 包含一个我们命名规范的概览。

卷 3 的简要指南

本卷有多种学习方法。任何从图 2 中标号为 1 的输入节点（即章）到标号为 32 的输出节点的路径都可以形成一个课程。让我们简要地阐述图 2 如下：

软件工程的基础课程： 最小的课程包括第 1、2、5、8、11、16、17、19、24~26、30~32 章，即图 2 的所有左边列章节。

领域工程： 集中讨论领域工程的课程另外包括第 9、10 与第 12~15 章。

需求工程： 集中讨论需求工程的课程除了基础课程之外还包括第 18 与第 20~23 章。

软件设计： 集中讨论软件设计的课程除了基础课程之外还包括第 27~29 章。

任一上面概述的四种课程可以以两种方式的任一一种给出：

非形式的： 以这种方式学习本卷的读者可以略过形式化部分而只关注非形式的材料。换言之，学习本卷基本上且实际上可以不先学习卷 1 或卷 1 与卷 2。

形式的： 以这种方式学习本卷的读者需要学习所有非形式及形式的材料——因此学习本卷的一个先决条件是至少先学习了卷 1。

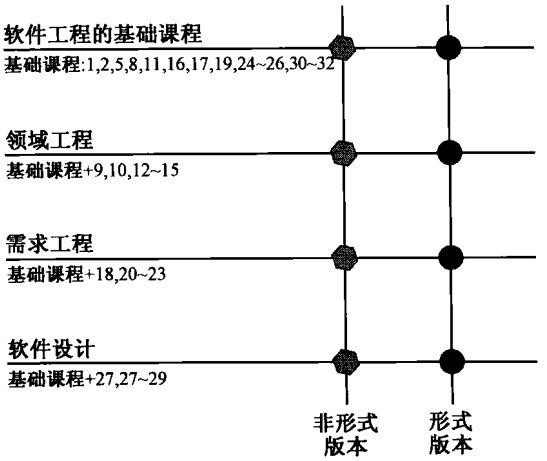


图. 1　课程选择

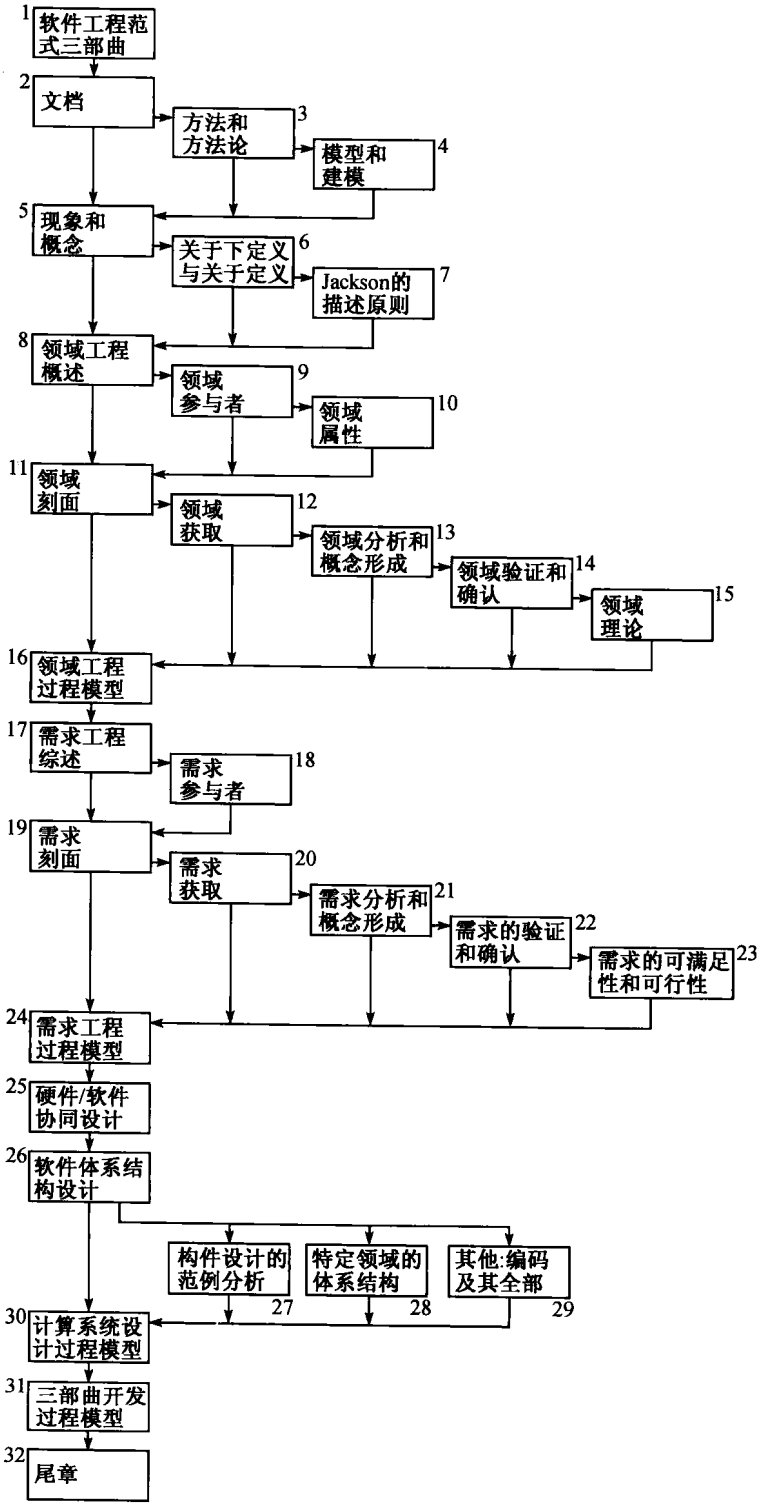
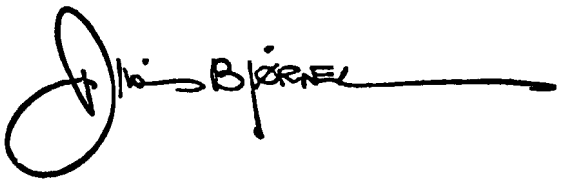


图. 2　课程优先图

致谢

卷 1 与卷 2 的致谢继续适用于本卷。此外，我希望对 Kirsten Mark Hansen 表示谢意，因为她允许我编辑她杰出的博士论文 [137] 的第 4 章作为本书第 19.6.5 节。再一次，我希望对过去近 30 年我学术快乐的主要源泉，即我的大学：丹麦技术大学，致以特别的谢意。



Dines Bjørner
丹麦技术大学，2005–2006

目录

III 描述：理论和实践