

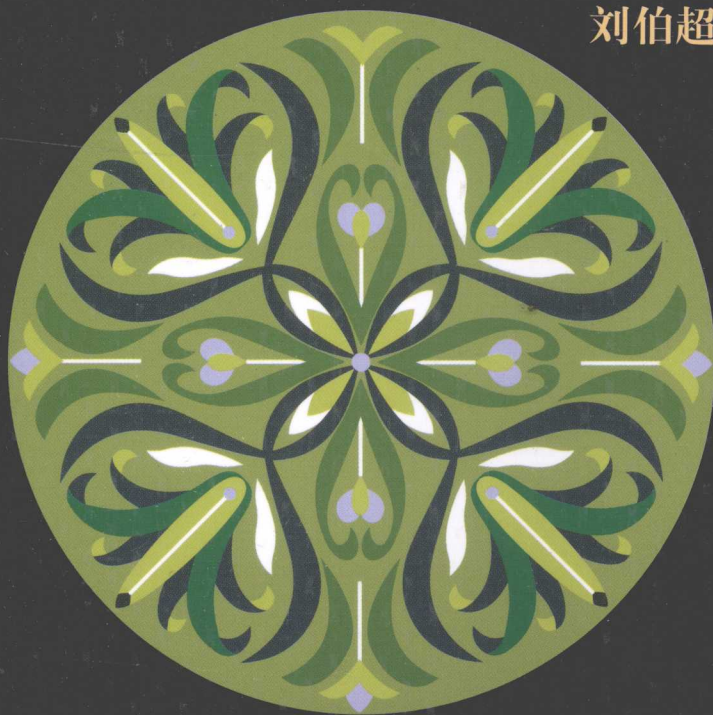
世界著名计算机教材精选

软件工程

卷2

系统与语言规约

Dines Bjørner 著
刘伯超 向剑文 等译



SOFTWARE ENGINEERING 2

Specification of Systems and Languages

清华大学出版社



世界著名计算机教材精选

Software Engineering 2

Specification of Systems and Languages

软件工程卷 2

系统与语言规约

Dines Bjørner 著

刘伯超 向剑文 等译

清华大学出版社

北 京

English reprint edition copyright © 2009 by Springer-Verlag and TSINGHUA UNIVERSITY PRESS.

Original English language title from Proprietor's edition of the Work.

Original English language title: Software Engineering 2: Specification of Systems and Languages by Dines

Bjørner, Copyright © 2009

All Rights Reserved.

This edition has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.

本书翻译版由 Springer-Verlag 授权给清华大学出版社出版发行。

北京市版权局著作权合同登记号 图字 01-2007-0336 号

本书封面贴有清华大学出版社防伪标签, 无标签者不得销售

版权所有, 侵权必究。侵权举报电话: 010-62782989 13701121933

图书在版编目(CIP)数据

软件工程卷 2: 系统与语言规约/ (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 2: Specification of Systems and Languages

ISBN 978-7-302-20891-4

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 159921 号

责任编辑: 龙啟铭

责任校对: 徐俊伟

责任印制: 何 芊

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 装 者: 清华大学印刷厂

经 销: 全国新华书店

开 本: 185×260 印 张: 42.25 字 数: 1053 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: 023237-01

Charlotte, Camilla 与 Caroline

我是否感激？当然！我是一个快乐的父亲吗？你所作的也一样！

黄色的树林里分出两条路，
可惜我不能同时去涉足，
我在那路口久久伫立，
我向着一条路极目望去，
直到它消失在丛林深处。

但我却选了另外一条路，
它荒草萋萋，十分幽寂，
显得更诱人、更美丽，
虽然在这两条小路上，
都很少留下旅人的足迹，

虽然那天清晨落叶满地，
两条路都未经脚印污染。
呵，留下一条路等改日再见！
但我知道路径延绵无尽头，
恐怕我难以再回返。

也许多少年后在某个地方，
我将轻声叹息把往事回顾，
一片树林里分出两条路，
而我选了人迹更少的一条，
从此决定了我一生的道路。

罗勃·佛洛斯特（Robert Frost）：未选择的路（1915） [119]
（人民文学出版社（1984）顾子欣译）

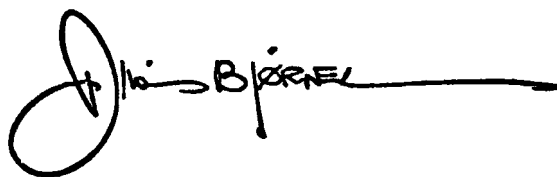
原著作者为中文版所作的序

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。

A handwritten signature in black ink, reading "Dines Bjørner". The signature is stylized, with a large loop at the beginning and a long horizontal line extending to the right.

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 1~3 章，刘伯超翻译了第 4~13 章、第 16~20 章以及附录 A，孔维强翻译了第 14~15 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。

序言

本卷是有关软件工程的工程原则与技术的三卷书中的第2卷。有关本丛书这几卷的一个适当的序言及总体介绍，请参阅第 1 卷的序言及该卷的第 1 章。我们假设读者已经学习了第 1 卷。

概述

本卷集中讨论对语言和系统进行规约的原则与技术。它使用在第 1 卷中介绍的抽象与建模原则、技术和工具，并且进一步补充了那些原则、技术和工具。本卷特别强调以下四个方面：

- 高级规约刻画：
 - ★ 层次和复合 第 2 章
 - ★ 指称和计算 第 3 章
 - ★ 格局：上下文和状态 第 4 章
 - ★ 时间、空间和空间/时间 第 5 章
 - ★ 模块化 第 10 章
 - ★ 自动机和机器 第 11 章
- 语言学：
 - ★ 语用 第 6 章
 - ★ 语义 第 7 章
 - ★ 句法 第 8 章
 - ★ 符号体系 第 9 章
- 并发与时态：
 - ★ 佩特里网 第 12 章
 - ★ 消息序列图与活序列图 第 13 章
 - ★ 状态图 第 14 章
 - ★ 时间的定量模型 第 15 章
- 解释器与编译器定义：
 - ★ SAL：简单应用式语言 第 16 章
 - ★ SIL：简单命令式语言 第 17 章

- ★ SMIL: 简单模块命令式语言
- ★ SPIL: 简单并行命令式语言

第 18 章
第 19 章

“UML”化的形式技术

在这里需要强调一些值得注意的特点。在并发方面,第 12~14 章,也举例说明了图解的规约,正如第 10.3 节(UML 类图)所作的那样。该材料同时举例说明了可以简单并优雅地包含(即通过 RSL 来使用)统一建模语言(UML [58,234,379,439])的流行特点。Christian Krog Madsen 是第 12~14 章的主要作者。

RAISE 规约语言: RSL

与第 1 卷一样,在本卷中我们大量使用 RSL。因此我们在第 1 章中插入一段 RSL 的入门材料——其他的材料请参阅 RAISE 的链接地址: [http:// www.iist.unu.edu/raise/](http://www.iist.unu.edu/raise/)。

致谢

第 1 卷的序言包含了一个详尽的致谢章节。

RSL 与佩特里网(第 12 章)、消息序列图或活序列图(第 13 章)以及状态图(第 14 章)的结合主要归功于 Christian Krog Madsen [314,315]。在此向 Christian 致以大量及真诚的感谢。RSL 与类似 UML 的类图(第 10.3 节)的结合主要归功于 Steffen Holmslykke [9,10]。同样的感谢亲切地致给 Steffen。Martin Pěnička 提供了例 12.8 (第 12.3.4 节)、例 14.7 (第 14.4.1 节)和例 14.8 (第 14.4.2 节),在此同样真诚地致以感谢。

新加坡国立大学的同事 Andrei Stefan 和 Yang ShaoFa 研究并校对了第 12~15 章。同作为主要人物的 Yang ShaoFa 一起,我决定设计了第 13.6 节中的 CTP (Communicating Transaction Processes, 通信事务进程)模型。十分感谢他们的意见及工作。

从 1976 年至今在丹麦技术大学的 30 年经历是我在学术上快乐的一个主要源泉。

最后但并非最不重要的,我对施普林格的编辑 Ronan Nugent 的巨大支持表示感谢。

第 2 卷的简要指南

这一卷有若干章节。这些章节被归类成几个部分。图 2 概括了一个这些章节中的优先关系。该图把学习该卷的建议顺序放在一起。

- 第 1 章被认为是学习任何章节的一个先决条件。
- 我们把一些部分分组组成虚线环绕的组 $A - E$ 。
- 组 A 由第 2~5 章所组成，可以以任何顺序进行学习。
- 组 B 由第 6~9 章所组成，应该按照 6、7、8 和 9 的顺序进行学习。
- 组 C 由第 10~11 章所组成，可以以任何顺序进行学习。
- 组 D 由第 12~15 章所组成，可以以任何顺序进行学习。第 14 章包含一个需要首先学习第 13 章的例子。
- 组 E 由第 16~19 章所组成，应该按照 16、17 和 18 的顺序进行学习。第 19 章可以在中间、之前或之后进行学习。最好在之后。
- 组 $A \sim E$ 可以以任意顺序进行学习。但是在第 15 章之前先学习第 5 章，在第 18 章之前先学习第 10 章，以及在组 E 之前先学习组 B 可能会有帮助。
- 学习第 20 章是没有害处的。
- 附录 A 包含一个我们的命名约定的综述。

在大多数章中有许多小节可以被略过。典型地是那些带有较大的例子或接近于章的结尾部分的小节。

教师或读者可以用这种方式组合成许多适当的课程。在图 1 中建议了一些这样的课程。

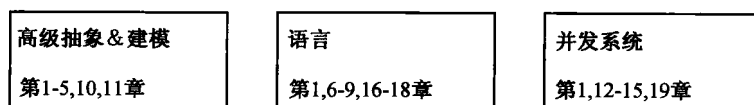
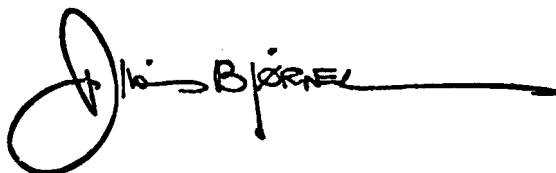


图1 仅基于第 2 卷的可供选择的课程



Dines Bjørner

丹麦技术大学，2005–2006

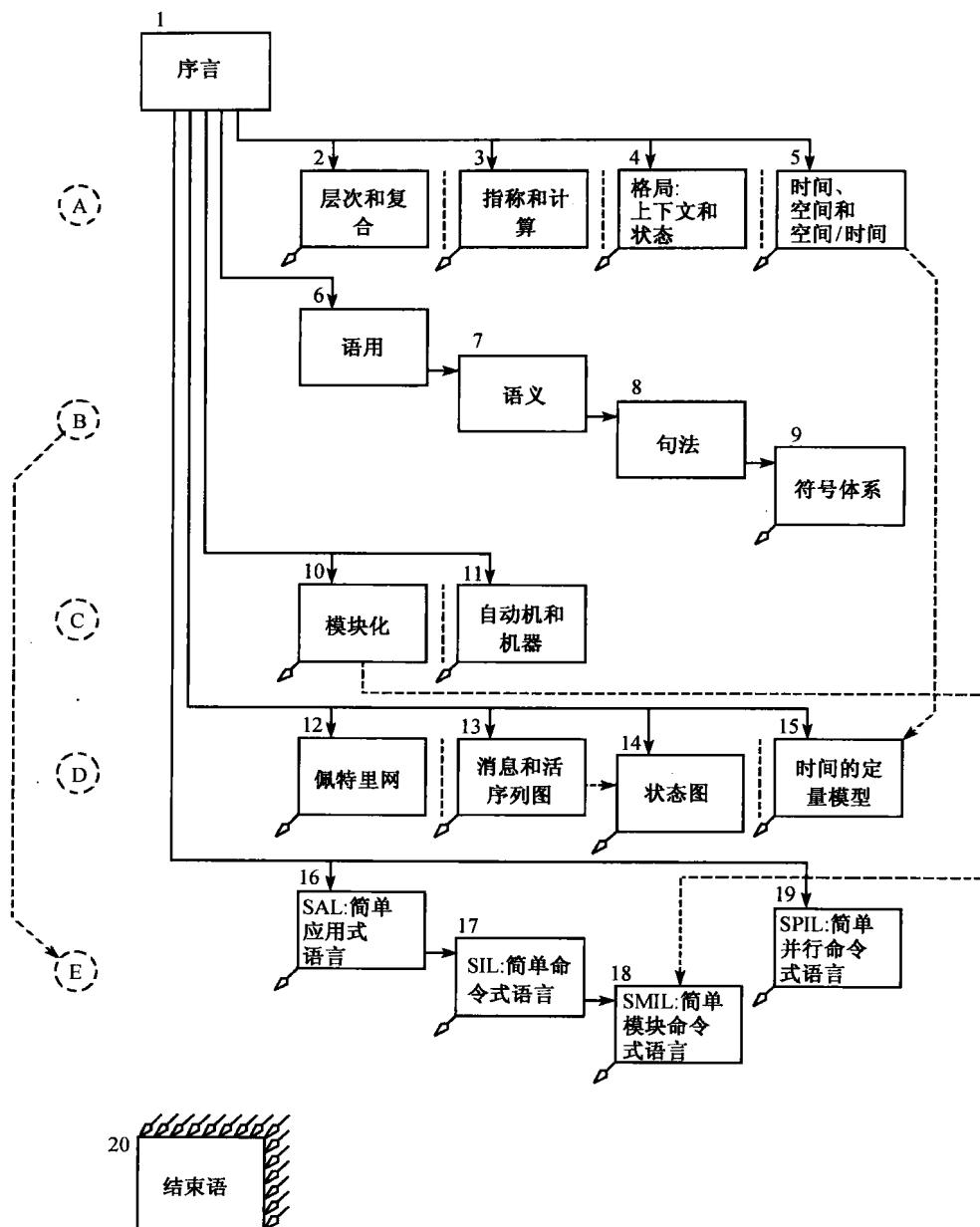


图2 章节优先次序图

目录

原著作者为中文版所作的序	v
译者序	vii

序言	ix
概述	ix
“UML”化的形式技术	x
RAISE 规约语言: RSL	x
致谢	x
第 2 卷的简要指南	xi

I 开篇

1 序言	3
1.1 前言	3
1.1.1 为什么有本卷	3
1.1.2 为什么要掌握这些原理、技术与工具	3
1.1.3 本卷“包含”了什么	4
1.1.4 本卷是如何“陈述”的	5
1.2 “轻量级”形式技术	5
1.3 RSL 的入门读物	7
1.3.1 类型	7
1.3.2 RSL 谓词演算	10
1.3.3 具体 RSL 类型	11
1.3.4 λ 演算 + 函数	19
1.3.5 其他应用表达式	21
1.3.6 命令式结构	24
1.3.7 进程结构	25
1.3.8 简单 RSL 规约	26

1.4 文献评注	27
----------------	----

II 规约刻画

2 层次与复合	31
2.1 关键问题	31
2.1.1 非形式说明	31
2.1.2 形式说明	32
2.2 初步的方法论的结论	33
2.2.1 一些定义	33
2.2.2 原则与技术	33
2.3 主要的例子	34
2.3.1 层次的叙述表示	34
2.3.2 层次的形式表示	36
2.3.3 复合的, 叙述性表示	39
2.3.4 复合的形式表示	41
2.4 讨论	43
2.5 文献评注: Stanisław Leshniewski	43
2.6 练习	43
3 指称和计算	47
3.1 前言	47
3.1.1 计算和指称	47
3.1.2 句法和语义	48
3.1.3 特性描述	48
3.2 指称语义	48
3.2.1 一个简单的例子: 数符	48
3.2.2 指称原则	49
3.2.3 表达式指称	50
3.2.4 GOTO 连续	53
3.2.5 指称语义的讨论	61
3.3 计算语义	63
3.3.1 关键问题	63
3.3.2 两个例子	63
3.3.3 表达式计算	63
3.3.4 GOTO 程序的计算语义	66
3.3.5 协同例程程序的计算语义	71
3.3.6 讨论	72
3.4 回顾: 指称和计算	73
3.5 一些语义的创始人	74

3.5.1	John McCarthy	74
3.5.2	Peter Landin	75
3.6	练习	76
4	格局: 上下文和状态	79
4.1	引言	80
4.2	问题	82
4.3	“现实世界”上下文和状态	83
4.3.1	物理系统: 上下文和状态	83
4.3.2	上下文和状态	84
4.3.3	非物理系统: 上下文和状态	84
4.3.4	讨论, I	85
4.3.5	讨论, II	86
4.4	第一次总结: 上下文和状态	86
4.4.1	概述	86
4.4.2	开发原则和技术	87
4.5	程序设计语言格局	87
4.6	并发进程格局	87
4.6.1	示例	87
4.6.2	总结	92
4.7	第二次总结: 上下文和状态	93
4.8	信息状态和行为状态	93
4.8.1	作为状态机数据的程序流程图	94
4.8.2	流程图 $\equiv$ 机器	94
4.8.3	流程图机	94
4.8.4	评论	95
4.8.5	结论	95
4.9	最后的总结: 上下文和状态	96
4.10	练习	97

III 关键领域和系统刻画

5	时间、空间和空间/时间	101
5.1	时间	101
5.1.1	时间——基础	102
5.1.2	时间——一般问题	104
5.1.3	时间的“A 序列”和“B 序列”模型	104
5.1.4	时间的连续统理论	105
5.1.5	时态事件	106
5.1.6	时态行为	106

5.1.7	时间表示	106
5.1.8	时间“上”的操作	108
5.2	空间	108
5.2.1	空间——基础	108
5.2.2	位置变化实体	109
5.2.3	位置和动态性	110
5.2.4	空间——一般问题	111
5.3	空间/时间	113
5.3.1	指导示例	113
5.3.2	空间/时间的表示	114
5.3.3	Blizard 的时间空间理论	114
5.4	讨论	115
5.5	文献评注	115
5.6	练习	115

IV 语言学

6	语用	121
6.1	前言	121
6.2	日常语用	122
6.3	“形式”语用	122
6.4	讨论	123
6.4.1	概述	123
6.4.2	原则和技术	123
6.5	文献评注	123
6.6	练习	124
7	语义	126
7.1	前言	126
7.2	具体语义	127
7.3	“抽象”语义	127
7.4	预备语义概念	127
7.4.1	句法和语义类型	127
7.4.2	上下文	128
7.4.3	状态	128
7.4.4	格局	128
7.4.5	解释、求值、细化	128
7.5	指称语义	129
7.5.1	简单情况	130
7.5.2	复合情况	130

7.6	宏扩展语义	130
7.6.1	重写	131
7.6.2	宏扩展	131
7.6.3	归纳重写	132
7.6.4	不动点求值	134
7.7	操作和计算语义	135
7.7.1	栈语义	135
7.7.2	属性语法语义	135
7.8	证明规则语义	139
7.9	讨论	141
7.9.1	概述	141
7.9.2	原则、技术和工具	141
7.10	文献评注	142
7.11	练习	142
8	句法	145
8.1	问题	145
8.1.1	形式和内容: 句法和语义	145
8.1.2	本章的结构和内容	146
8.2	句子和语义结构	146
8.2.1	概述	147
8.2.2	句子结构示例	147
8.2.3	语义结构示例	149
8.3	第一个抽象句法, John McCarthy	152
8.3.1	分析语法: 观测器和选择器	152
8.3.2	合成语法: 生成器	153
8.4	BNF 语法 $\approx$ 具体句法	153
8.4.1	BNF 语法	154
8.4.2	BNF $\leftrightarrow$ RSL 语法解析树关系	154
8.5	结构生成器和识别器	156
8.5.1	上下文无关语法和语言	156
8.5.2	语法解析树	157
8.5.3	正则表达式和语言	159
8.5.4	语言识别器	160
8.6	XML: 可扩展标记语言 (Extensible Markup Language)	160
8.6.1	例	160
8.6.2	讨论	162
8.6.3	历史背景	162
8.6.4	目前的 XML “狂热”	162
8.6.5	XML 表达式	162

8.6.6	XML 模式	164
8.6.7	参考	166
8.7	抽象句法	166
8.7.1	存储模型的抽象句法	166
8.7.2	其他存储模型的抽象句法	169
8.8	转换 RSL 类型到 BNF	170
8.8.1	问题	170
8.8.2	可能的解决办法	171
8.9	非形式和形式句法讨论	172
8.9.1	概述	172
8.9.2	原则、技术和工具	172
8.10	文献评注	173
8.11	练习	173
9	符号体系	180
9.1	符号体系= 句法 $\oplus$ 语义 $\oplus$ 语用	180
9.2	符号体系	181
9.3	语言构件	181
9.4	语言学	182
9.5	语言和系统	183
9.5.1	职业语言	183
9.5.2	元语言	184
9.5.3	系统	184
9.5.4	系统图语言	195
9.5.5	系统概念讨论	196
9.5.6	作为语言的系统	196
9.6	讨论	197
9.6.1	概述	197
9.6.2	原则、技术和工具	197
9.7	Charles Sanders Peirce	197
9.8	文献评注	197
9.9	练习	198

V 其他规约技术

10	模块化	205
10.1	前言	206
10.1.1	一些示例	206
10.1.2	预备性讨论	211
10.1.3	章节结构	213