

DESIGN AND VALIDATION OF COMPUTER PROTOCOLS

Gerard J. Holzmann

*Bell Laboratories
Murray Hill, New Jersey 07974*

PRENTICE-HALL
Englewood Cliffs, New Jersey 07632

Prentice Hall Software Series

Brian W. Kernighan, Advisor

Copyright © 1991 by Lucent Technologies, Bell Laboratories, Incorporated.

This book is typeset in Times Roman by the author,
using an Linotronic 200P phototypesetter and a DEC VAX 8550
running the 10th Edition of the UNIX® operating system.

DEC and VAX are trademarks of Digital Equipment Corporation.

UNIX is a registered trademark of AT&T.

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system,
or transmitted, in any form or by any means, electronic,
mechanical, photocopying, recording, or otherwise,
without the prior written permission of the publisher.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Prentice-Hall International (UK) Limited, *London*

Prentice-Hall of Australia Pty. Limited, *Sydney*

Prentice-Hall Canada Inc., *Toronto*

Prentice-Hall Hispanoamericana, S.A., *Mexico*

Prentice-Hall of India Private Limited, *New Delhi*

Prentice-Hall of Japan, Inc., *Tokyo*

Simon & Schuster Asia Pte. Ltd., *Singapore*

Editora Prentice-Hall do Brasil, Ltda., *Rio de Janeiro*

CONTENTS

Foreword	ix
Preface	xi
Part I — Basics	
1. Introduction	
1.1 Early Beginnings	1
1.2 The First Networks	9
1.3 Protocols as Languages	12
1.4 Protocol Standardization	13
1.5 Summary	15
Exercises	16
Bibliographic Notes	16
2. Protocol Structure	
2.1 Introduction	19
2.2 The Five Elements of a Protocol	21
2.3 An Example	22
2.4 Service and Environment	26
2.5 Vocabulary and Format	32
2.6 Procedure Rules	35
2.7 Structured Protocol Design	35
2.8 Ten Rules of Design	38
2.9 Summary	39
Exercises	39
Bibliographic Notes	40
3. Error Control	
3.1 Introduction	43
3.2 Error Model	44
3.3 Types of Transmission Errors	46
3.4 Redundancy	46
3.5 Types of Codes	47
3.6 Parity Check	48
3.7 Error Correction	48
3.8 A Linear Block Code	52
3.9 Cyclic Redundancy Checks	56

3.10	Arithmetic Checksum	63
3.11	Summary	64
	Exercises	64
	Bibliographic Notes	65
4.	Flow Control	
4.1	Introduction	66
4.2	Window Protocols	70
4.3	Sequence Numbers	74
4.4	Negative Acknowledgments	80
4.5	Congestion Avoidance	83
4.6	Summary	86
	Exercises	87
	Bibliographic Notes	88

Part II — Specification and Modeling

5.	Validation Models	
5.1	Introduction	90
5.2	Processes, Channels, Variables	91
5.3	Executability of Statements	91
5.4	Variables and Data Types	92
5.5	Process Types	93
5.6	Message Channels	96
5.7	Control Flow	100
5.8	Examples	102
5.9	Modeling Procedures and Recursion	104
5.10	Message Type Definitions	104
5.11	Modeling Timeouts	105
5.12	Lynch's Protocol Revisited	106
5.13	Summary	107
	Exercises	108
	Bibliographic Notes	109
6.	Correctness Requirements	
6.1	Introduction	111
6.2	Reasoning about Behavior	112
6.3	Assertions	114
6.4	System Invariants	115
6.5	Deadlocks	117
6.6	Bad Cycles	118
6.7	Temporal Claims	119
6.8	Summary	125
	Exercises	126
	Bibliographic Notes	127
7.	Protocol Design	
7.1	Introduction	128

7.2	Service Specification	129
7.3	Assumptions about the Channel	130
7.4	Protocol Vocabulary	131
7.5	Message Format	133
7.6	Procedure Rules	140
7.7	Summary	160
	Exercises	160
	Bibliographic Notes	161
8.	Finite State Machines	
8.1	Introduction	162
8.2	Informal Description	162
8.3	Formal Description	169
8.4	Execution of Machines	170
8.5	Minimization of Machines	171
8.6	The Conformance Testing Problem	174
8.7	Combining Machines	175
8.8	Extended Finite State Machines	176
8.9	Generalization of Machines	178
8.10	Restricted Models	181
8.11	Summary	184
	Exercises	185
	Bibliographic Notes	185

Part III — Conformance Testing, Synthesis and Validation

9.	Conformance Testing	
9.1	Introduction	187
9.2	Functional Testing	188
9.3	Structural Testing	189
9.4	Deriving UIO Sequences	195
9.5	Modified Transition Tours	196
9.6	An Alternative Method	197
9.7	Summary	199
	Exercises	200
	Bibliographic Notes	200
10.	Protocol Synthesis	
10.1	Introduction	203
10.2	Protocol Derivation	203
10.3	Derivation Algorithm	208
10.4	Incremental Design	210
10.5	Place Synchronization	210
10.6	Summary	211
	Exercises	212
	Bibliographic Notes	212
11.	Protocol Validation	

11.1	Introduction	214
11.2	Manual Proof Method	214
11.3	Automated Validation Methods	218
11.4	The Supertrace Algorithm	226
11.5	Detecting Non-Progress Cycles	231
11.6	Detecting Acceptance Cycles	234
11.7	Checking Temporal Claims	235
11.8	Complexity Management	235
11.9	Boundedness of PROMELA Models	237
11.10	Summary	238
	Exercises	239
	Bibliographic Notes	240

Part IV — Design Tools

12.	A Protocol Simulator	
12.1	Introduction	243
12.2	SPIN — Overview	244
12.3	Expressions	245
12.4	Variables	255
12.5	Statements	265
12.6	Control Flow	275
12.7	Process and Message Types	282
12.8	Macro Expansion	292
12.9	SPIN Options	293
12.10	Summary	294
	Exercises	295
	Bibliographic Notes	296
13.	A Protocol Validator	
13.1	Introduction	297
13.2	Structure of the Validator	298
13.3	The Validation Kernel	299
13.4	The Transition Matrix	302
13.5	The Validator-Generator Code	303
13.6	Overview of the Code	306
13.7	Guided Simulation	308
13.8	Some Applications	310
13.9	Coverage in Supertrace Mode	315
13.10	Summary	316
	Exercises	316
	Bibliographic Notes	317

14. Using the Validator	
14.1 Introduction	318
14.2 An Optical Telegraph Protocol	318
14.3 Dekker's Algorithm	320
14.4 A Larger Validation	322
14.5 Flow Control Validation	325
14.6 Session Layer Validation	336
14.7 Summary	349
Exercises	349
Bibliographic Notes	349
Conclusion	351
References	352
Appendices	
A. Data Transmission	367
B. Flow Chart Language	380
C. PROMELA Language Report	383
D. SPIN Simulator Source	393
E. SPIN Validator Source	436
F. PROMELA File Transfer Protocol	528
Name Index	537
Subject Index	539

