DESIGN AND VALIDATION
OF COMPUTER PROTOCOLS

Gerard J. Holzmann
Bell Laboratories
Murray Hill, New Jersey 07974
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
# Part III — Conformance Testing, Synthesis and Validation

## 9. Conformance Testing

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Introduction</td>
<td>187</td>
</tr>
<tr>
<td>9.2 Functional Testing</td>
<td>188</td>
</tr>
<tr>
<td>9.3 Structural Testing</td>
<td>189</td>
</tr>
<tr>
<td>9.4 Deriving UIO Sequences</td>
<td>195</td>
</tr>
<tr>
<td>9.5 Modified Transition Tours</td>
<td>196</td>
</tr>
<tr>
<td>9.6 An Alternative Method</td>
<td>197</td>
</tr>
<tr>
<td>9.7 Summary</td>
<td>199</td>
</tr>
<tr>
<td>Exercises</td>
<td>200</td>
</tr>
<tr>
<td>Bibliographic Notes</td>
<td>200</td>
</tr>
</tbody>
</table>

## 10. Protocol Synthesis

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1 Introduction</td>
<td>203</td>
</tr>
<tr>
<td>10.2 Protocol Derivation</td>
<td>203</td>
</tr>
<tr>
<td>10.3 Derivation Algorithm</td>
<td>208</td>
</tr>
<tr>
<td>10.4 Incremental Design</td>
<td>210</td>
</tr>
<tr>
<td>10.5 Place Synchronization</td>
<td>210</td>
</tr>
<tr>
<td>10.6 Summary</td>
<td>211</td>
</tr>
<tr>
<td>Exercises</td>
<td>212</td>
</tr>
<tr>
<td>Bibliographic Notes</td>
<td>212</td>
</tr>
</tbody>
</table>

## 11. Protocol Validation
14. Using the Validator

14.1 Introduction

14.2 An Optical Telegraph Protocol

14.3 Dekker’s Algorithm

14.4 A Larger Validation

14.5 Flow Control Validation

14.6 Session Layer Validation

14.7 Summary

Exercises

Bibliographic Notes

| 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 |