Contents

"If you don't know where you're going,
it doesn't really matter which path you take."
(Lewis Carroll, 1832–1898)

Preface ix

Introduction

1 Finding Bugs in Concurrent Systems 1
Circular Blocking, Deadly Embrace, Mismatched Assumptions, Fundamental Problems of Concurrency, Observability and Controllability

2 Building Verification Models 7
Introducing PROMELA, Some Examples, Biographical Notes

3 An Overview of PROMELA 33
Processes, Data Objects, Message Channels, Channel Poll Operations, Sorted Send and Random Receive, Rendezvous Communication, Rules for Executability, Control Flow, Finding out More

4 Defining Correctness Claims 73
Basic Types of Claims, Assertions, Meta-Labels, Fair Cycles, Never Claims, The Link with LTL, Trace Assertions, Predefined Variables and Functions, Path Quantification, Finding out More

5 Using Design Abstraction 101
What Makes a Good Design Abstraction?, Data and Control, The Smallest Sufficient Model, Avoiding Redundancy, Counters, Sinks, Sources, and Filters, Simple Refutation Models, Examples, Controlling Complexity, A Formal Basis for Reduction

Foundation

6 Automata and Logic 127

Omega Acceptance, The Stutter Extension Rule, Finite States, Infinite Runs, Other Types of Acceptance, Temporal Logic, Recurrence and Stability, Valuation Sequences, Stutter Invariance, Fairness, From Logic to Automata, Omega-Regular Properties, Other Logics, Bibliographic Notes

7 PROMELA Semantics 153

Transition Relation, Operational Model, Semantics Engine, Interpreting PROMELA Models, Three Examples, Verification, The Never Claim

8 Search Algorithms 167

Depth-First Search, Checking Safety Properties, Depth-Limited Search, Trade-Offs, Breath-First Search, Checking Liveness Properties, Adding Fairness, The SPIN Implementation, Complexity Revisited, Bibliographic Notes

9 Search Optimization 191

Partial Order Reduction, Visibility, Statement Merging, State Compression, Collapse Compression, The Minimized Automaton Representation, Bitstate Hashing, Bloom Filters, Hash-Compact, Bibliographic Notes

10 Notes on Model Extraction 217

The Role of Abstraction, From ANSI-C to PROMELA, Embedded Assertions, A Framework for Abstraction, Soundness and Completeness, Selective Data Hiding, Bolder Abstractions, Dealing with False Negatives, Thorny Issues with Embedded C Code, The Model Extraction Process, The Halting Problem Revisited, Bibliographic Notes

Practice

11 Using SPIN 245

SPIN Structure, Roadmap, Random Simulation, Interactive Simulation, Generating and Compiling a Verifier, Tuning a Verification Run, the Number of Reachable States, Search Depth, Cycle Detection, Inspecting Error Traces, Internal State Numbers, Special Cases, Disabling Partial Order Reduction, Boosting Performance, Separate Compilation, Lowering Verification Complexity

12 Notes on XSPIN 267

Starting a Session with XSPIN, Menus, Syntax Checking, Property-Based Slicing, Simulation Parameters, Verification Parameters, The LTL Property Manager, The Automaton View Option

13 The TimeLine Editor 283

An Example, Types of Events, Defining Events, Matching a Timeline, Automata Definitions, Variations on a Theme, Constraints, Timelines with One Event, Timelines with Multiple Events, The Link with LTL, Bibliographic Notes

14 A Verification Model of a Telephone Switch 299

General Approach, Keeping it Simple, Managing Complexity, Subscriber Model, Switch Model, Remote Switches, Adding Features, Three-Way Calling

15 Sample SPIN Models 325

The Sieve of Eratosthenes, Process Scheduling, A Client-Server Model, A Square-Root Server, Adding Interaction, Adding Assertions, A Comment Filter

Reference Material

16 PROMELA Language Reference 363

Grammar Rules, Special Cases, PROMELA Manual Pages, Meta Terms, Declarators, Control Flow Constructors, Basic Statements, Predefined Functions and Operators, Omissions

17 Embedded C Code 495

Example, Data References, Execution, Issues to Consider, Deferring File Inclusion, Manual Pages for Embedded C Code

18 Overview of SPIN Options 513

Compile-Time Options, Simulation, Syntax-Checking, Postscript Generation, Model Checker Generation, LTL Conversion, Miscellaneous Options

19 Overview of PAN Options 527

PAN Compile-Time Options, Tuning Partial Order Reduction, Increasing Speed, Decreasing Memory Use, Debugging PAN Verifiers, Experimental Options, PAN Run-Time Options, PAN Output Format

Literature 545

Appendices

A Automata Products 553

Asynchronous and Synchronous Products, Defining Atomic Sequences and Rendezvous, Expanded Asynchronous Products, Büchi Acceptance, Non-Progress, Deadlock

B The Great Debates 563

Branching vs Linear Time, Symbolic vs Explicit, Breadth-First vs Depth-First, Tarjan vs Nested, Events vs States, Realtime vs Timeless, Probability vs Possibility, Asynchronous vs Synchronous, Interleaving vs True Concurrency, Open vs Closed Systems

C Exercises with SPIN 573

D Downloading SPIN 579

Tables and Figures 581

Index 585

> *"You got to be careful if you don't know where you're going, because you might not get there."*
> *(Yogi Berra, 1925–)*