Contents

Part I. Principles and Techniques

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Automata</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Introductory Examples</td>
<td>5</td>
</tr>
<tr>
<td>1.2</td>
<td>A Few Definitions</td>
<td>5</td>
</tr>
<tr>
<td>1.3</td>
<td>A Printer Manager</td>
<td>9</td>
</tr>
<tr>
<td>1.4</td>
<td>A Few More Variables</td>
<td>11</td>
</tr>
<tr>
<td>1.5</td>
<td>Synchronized Product</td>
<td>12</td>
</tr>
<tr>
<td>1.6</td>
<td>Synchronization by Message Passing</td>
<td>14</td>
</tr>
<tr>
<td>1.7</td>
<td>Synchronization by Shared Variables</td>
<td>21</td>
</tr>
<tr>
<td>2.</td>
<td>Temporal Logic</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>The Language of Temporal Logic</td>
<td>27</td>
</tr>
<tr>
<td>2.2</td>
<td>The Formal Syntax of Temporal Logic</td>
<td>28</td>
</tr>
<tr>
<td>2.3</td>
<td>The Semantics of Temporal Logic</td>
<td>32</td>
</tr>
<tr>
<td>2.4</td>
<td>PLTL and CTL: Two Temporal Logics</td>
<td>33</td>
</tr>
<tr>
<td>2.5</td>
<td>The Expressivity of CTL*</td>
<td>35</td>
</tr>
<tr>
<td>3.</td>
<td>Model Checking</td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Model Checking CTL</td>
<td>39</td>
</tr>
<tr>
<td>3.2</td>
<td>Model Checking PLTL</td>
<td>42</td>
</tr>
<tr>
<td>3.3</td>
<td>The State Explosion Problem</td>
<td>45</td>
</tr>
<tr>
<td>4.</td>
<td>Symbolic Model Checking</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Symbolic Computation of State Sets</td>
<td>47</td>
</tr>
<tr>
<td>4.2</td>
<td>Binary Decision Diagrams (BDD)</td>
<td>47</td>
</tr>
<tr>
<td>4.3</td>
<td>Representing Automata by BDDs</td>
<td>51</td>
</tr>
<tr>
<td>4.4</td>
<td>BDD-based Model Checking</td>
<td>54</td>
</tr>
<tr>
<td>5.</td>
<td>Timed Automata</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Description of a Timed Automaton</td>
<td>59</td>
</tr>
<tr>
<td>5.2</td>
<td>Networks of Timed Automata and Synchronization</td>
<td>60</td>
</tr>
</tbody>
</table>
5.3 Variants and Extensions of the Basic Model ......................... 64
5.4 Timed Temporal Logic ............................................. 67
5.5 Timed Model Checking ............................................. 68

Conclusion ................................................................. 73

Part II. Specifying with Temporal Logic

Introduction ............................................................... 77

6. Reachability Properties ................................................ 79
   6.1 Reachability in Temporal Logic .................................. 79
   6.2 Model Checkers and Reachability ............................... 80
   6.3 Computation of the Reachability Graph ...................... 80

7. Safety Properties ...................................................... 83
   7.1 Safety Properties in Temporal Logic .......................... 83
   7.2 A Formal Definition ............................................. 84
   7.3 Safety Properties in Practice .................................. 86
   7.4 The History Variables Method ................................. 87

8. Liveness Properties .................................................... 91
   8.1 Simple Liveness in Temporal Logic ............................ 92
   8.2 Are Liveness Properties Useful? ............................... 92
   8.3 Liveness in the Model, Liveness in the Properties .......... 94
   8.4 Verification under Liveness Hypotheses ...................... 96
   8.5 Bounded Liveness ............................................... 97

9. Deadlock-freeness ..................................................... 99
   9.1 Safety? Liveness? ................................................. 99
   9.2 Deadlock-freeness for a Given Automaton ................... 99
   9.3 Beware of Abstractions! ....................................... 101

10. Fairness Properties .................................................. 103
    10.1 Fairness in Temporal Logic .................................. 103
    10.2 Fairness and Nondeterminism ................................ 104
    10.3 Fairness Properties and Fairness Hypotheses .............. 104
    10.4 Strong Fairness and Weak Fairness .......................... 106
    10.5 Fairness in the Model or in the Property? ................ 107

11. Abstraction Methods ................................................ 109
    11.1 When Is Model Abstraction Required? ...................... 110
    11.2 Abstraction by State Merging ............................... 110
    11.3 What Can Be Proved in the Abstract Automaton? .......... 110
    11.4 Abstraction on the Variables ............................... 114
11.5 Abstraction by Restriction ........................................... 118
11.6 Observer Automata .................................................... 120

Conclusion ........................................................................ 125

Part III. Some Tools

Introduction ....................................................................... 129

12. SMV – Symbolic Model Checking .................................... 131
  12.1 What Can We Do with SMV? ........................................ 131
  12.2 SMV’s Essentials ..................................................... 131
  12.3 Describing Automata .................................................. 132
  12.4 Verification .............................................................. 135
  12.5 Synchronizing Automata ............................................. 136
  12.6 Documentation and Case Studies ............................... 137
  SMV Bibliography .......................................................... 138

13. SPIN – Communicating Automata .................................. 139
  13.1 What Can We Do with SPIN? ...................................... 139
  13.2 SPIN’s Essentials ..................................................... 139
  13.3 Describing Processes ................................................ 140
  13.4 Simulating the System .............................................. 141
  13.5 Verification .............................................................. 142
  13.6 Documentation and Case Studies ............................... 144
  SPIN Bibliography .......................................................... 144

14. DESIGN/CPN – Coloured Petri Nets ............................. 145
  14.1 What Can We Do with DESIGN/CPN? ......................... 145
  14.2 DESIGN/CPN’s Essentials ........................................ 145
  14.3 Editing with DESIGN/CPN ........................................ 146
  14.4 Simulating the Net ................................................... 147
  14.5 Analyzing the Net ..................................................... 149
  14.6 Documentation and Case Studies ............................... 149
  DESIGN/CPN Bibliography .............................................. 150

15. UPPAAL – Timed Systems ............................................ 153
  15.1 What Can We Do with UPPAAL? ............................... 153
  15.2 UPPAAL’s Essentials ................................................ 153
  15.3 Modeling Timed Systems with UPPAAL ....................... 154
  15.4 Simulating a System ................................................ 157
  15.5 Verification .............................................................. 157
  15.6 Documentation and Case Studies ............................... 158
  UPPAAL Bibliography ..................................................... 158
16. KRONOS – Model Checking of Real-time Systems ...... 161
   16.1 What Can We Do with KRONOS? ...................... 161
   16.2 KRONOS’ Essentials ................................ 161
   16.3 Describing Automata .................................. 162
   16.4 Synchronized Product ................................. 164
   16.5 Model Checking ....................................... 165
   16.6 Documentation and Case Studies .................... 167
KRONOS Bibliography ....................................... 167

17. HYTECH – Linear Hybrid Systems ....................... 169
   17.1 What Can We Do With HYTECH? ...................... 169
   17.2 HYTECH’s Essentials ................................ 169
   17.3 Describing Automata .................................. 170
   17.4 System Analysis ...................................... 172
   17.5 Parametric Analysis .................................. 174
   17.6 Documentation and Case Studies .................... 176
HYTECH Bibliography ...................................... 176

Main Bibliography .......................................... 179

Index .......................................................... 183