## Contents

1 Introduction .................................................................. 1
   1.1 Invariance Examples .................................................... 2
      1.1.1 A Chess Board Problem ....................................... 2
      1.1.2 A Black and White Balls Game .............................. 4
   1.2 The Way Ahead ......................................................... 5

2 Background ................................................................... 7
   2.1 Predicates ................................................................ 8
      2.1.1 Propositional Calculus ........................................ 8
      2.1.2 Predicate Calculus ............................................. 10
      2.1.3 Predicates Define Sets of States .............................. 10
      2.1.4 Strong and Weak Predicates ................................. 11
   2.2 Specifying Pre- and Postconditions ................................. 14
      2.2.1 Hoare Triples as Specifications of Total Correctness ........ 14
      2.2.2 Weakest Preconditions and Semantics ....................... 16
   2.3 Guarded Command Language .......................................... 17
      2.3.1 Empty Command .............................................. 18
      2.3.2 Diversion: Some Extreme Cases .............................. 18
      2.3.3 Assignment .................................................... 24
      2.3.4 Composition ................................................... 27
      2.3.5 Selection ....................................................... 30
      2.3.6 Repetition ...................................................... 32
   2.4 Refinement Rules ....................................................... 34
      2.4.1 Strengthen Postcondition Rule ................................. 35
      2.4.2 Weaken Precondition Rule .................................... 36
      2.4.3 Skip Rule ...................................................... 36
      2.4.4 Sequences of Refinements ................................. 37
      2.4.5 Refinement and Weakest Preconditions ...................... 37
      2.4.6 Assignment Rule .............................................. 37
      2.4.7 Composition Rule ............................................. 38
      2.4.8 Following Assignment Rule ................................. 40
## 4 Intermediary Examples

### 4.1 Dutch National Flag

- **Formulating the Problem** ..................................................... 96
- **Choosing the Invariant** ..................................................... 98
- **Refining the Specification** .................................................. 99
- **Proving the Third Guard Command** .......................... 100
- **Putting it All Together** ..................................................... 102
- **Discussion** ..................................................... 102

### 4.2 Longest Segment

- **Formulating the Problem** ..................................................... 104
- **A First Attempt at Refinement** ........................................ 105
- **A Revised Attempt at Refinement** ............................ 107
- **Putting it All Together** ..................................................... 111
- **Discussion** ..................................................... 112

### 4.3 Palindromes

- **The Outer Loop** ..................................................... 113
- **Formulating the Problem** ..................................................... 113
- **Refining the Specification** .................................................. 115
- **Putting it All Together** ..................................................... 116
- **Discussion** ..................................................... 117

### 4.4 Raster Lines

- **Formulating the Problem** ..................................................... 118
- **Deriving the Loop** ..................................................... 121
- **Developing the Loop’s Body** ........................................ 122
- **Putting it All Together** ..................................................... 125
- **Discussion** ..................................................... 126

### 4.5 Raster Circle

- **Problem Statement** ..................................................... 127
- **From Invariant to Loop** ..................................................... 129
- **Refining the Loop’s Body** ........................................ 129
- **Determining the Guards** .................................................. 132
- **Deriving the Guards** ..................................................... 133
- **Putting it All Together** ..................................................... 134

### 4.6 Majority Voting

- **Formulating the Problem** ..................................................... 137
- **Arriving at an Invariant and Developing the Loop** ........... 138
- **Developing the Guards** ..................................................... 139
- **Discussion** ..................................................... 143

### 4.7 Computational Geometry

- **Background and Notation** .................................................. 144
- **The Approach to Solving the Problem** .................................. 146
- **Deriving the Solution Constructively** ............................ 147
- **Discussion** ..................................................... 150

### 4.8 Revision Exercises

- ................................................................. 151
5 Procedures and Recursion .................................................. 161
  5.1 Introduction ............................................................. 161
5.2 Procedures ............................................................... 162
  5.2.1 Parameterless Procedures ..................................... 162
  5.2.2 Pass by Value .................................................. 164
  5.2.3 Pass by Result ................................................. 167
  5.2.4 Pass by Value Result .......................................... 168
  5.2.5 Functions ...................................................... 169
5.3 Procedure Refinement Strategy ........................................ 170
5.4 Recursive Procedures ................................................... 171
5.5 Terminating Recursive Programs ..................................... 173
5.6 Recursive Examples ..................................................... 177
  5.6.1 Factorial........................................................ 177
  5.6.2 Searching a List ............................................... 181
  5.6.3 Evaluating an Expression Tree ................................ 185
  5.6.4 MergeSort...................................................... 191
5.7 Conclusion .............................................................. 194

6 Case Study: Lattice Cover Graph Construction ......................... 197
  6.1 Introduction ............................................................. 197
  6.2 Preliminaries ............................................................ 198
    6.2.1 Lattices ......................................................... 198
    6.2.2 Set Intersection-Closed Lattices .............................. 201
  6.3 The Algorithm ........................................................... 205
    6.3.1 The Basic Structure ........................................... 206
    6.3.2 Articulating and Attaining $inv1(i)$ .......................... 207
    6.3.3 Articulating and Attaining $inv2(i)$ ....................... 208
    6.3.4 Filling in $S_1$ .................................................. 210
    6.3.5 Completing the Select Command ............................. 211
    6.3.6 The Completed Algorithm .................................... 214
    6.3.7 The Operational Implications ................................. 215
  6.4 Refactoring ............................................................. 218
    6.4.1 Efficiently Inserting $C_i \cap X$ ............................ 218
    6.4.2 Finding the Parent of $X$ ................................. 219
    6.4.3 Discussion ..................................................... 221
  6.5 A Gentle Introduction to Formal Concept Analysis ............... 222

7 Case Study 2: Classifying MADFA Construction Algorithms .......... 227
  7.1 Introduction ............................................................. 227
  7.2 From DFAs to MADFAs ................................................ 228
    7.2.1 Deterministic Finite Automata—DFAs ....................... 228
    7.2.2 Acyclic Deterministic Finite Automata—ADFAs ............ 230
    7.2.3 Minimum Acyclic Deterministic Finite Automata—MADFAs .... 231
    7.2.4 Concepts for MADFA Construction Algorithms ............ 232
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3 An Abstract MADFA Construction Algorithm</td>
<td>237</td>
</tr>
<tr>
<td>7.3.1 Structural Invariant Instantiations</td>
<td>239</td>
</tr>
<tr>
<td>7.3.2 The Procedures to be Instantiated</td>
<td>241</td>
</tr>
<tr>
<td>7.3.3 The Importance of the Skeleton-Based Taxonomy</td>
<td>241</td>
</tr>
<tr>
<td>7.4 Trie Intermediate ADFA</td>
<td>242</td>
</tr>
<tr>
<td>7.4.1 Procedure add_word_T</td>
<td>242</td>
</tr>
<tr>
<td>7.4.2 Adding Only Prefix Words</td>
<td>244</td>
</tr>
<tr>
<td>7.4.3 Adding a Non-prefix Word in a Trie</td>
<td>244</td>
</tr>
<tr>
<td>7.4.4 Procedure cleanup_T</td>
<td>246</td>
</tr>
<tr>
<td>7.4.5 An Example</td>
<td>249</td>
</tr>
<tr>
<td>7.5 Arbitrary Intermediate ADFA</td>
<td>250</td>
</tr>
<tr>
<td>7.5.1 Procedure add_word_N</td>
<td>251</td>
</tr>
<tr>
<td>7.5.2 Procedure cleanup_N</td>
<td>255</td>
</tr>
<tr>
<td>7.5.3 Commentary</td>
<td>255</td>
</tr>
<tr>
<td>7.6 Word Adding Based on a Partial Order</td>
<td>255</td>
</tr>
</tbody>
</table>

References 259

Index 263
The Correctness-by-Construction Approach to Programming
Kourie, D.G.; Watson, B.W.
2012, XIV, 266 p., Hardcover
ISBN: 978-3-642-27918-8