Contents

Version Abregée **vii**

Abstract **ix**

Acknowledgements **xi**

1 Introduction **1**
- 1.1 Scope of the Thesis 4
- 1.2 Contributions 5
- 1.3 Chapter Outline 5

2 Background **7**
- 2.1 Words and Languages 7
- 2.2 Transition Systems 8
  - 2.2.1 Basic Transition Systems 8
  - 2.2.2 Fair Transition Systems 9
- 2.3 Syntactic Representation 11
  - 2.3.1 Assertion language 11
  - 2.3.2 System Specifications 12
- 2.4 Temporal Logic 13
  - 2.4.1 Syntax 13
  - 2.4.2 Semantics 15
  - 2.4.3 Ground-quantified CTL* 18
  - 2.4.4 The Model Checking Problem 18
- 2.5 Algorithmic Model Checking 18
  - 2.5.1 The Automata-theoretic Approach 19
  - 2.5.2 Local Model Checking 19
  - 2.5.3 Symbolic Model Checking 20
  - 2.5.4 Reduction Techniques 20
- 2.6 Deductive Approaches to Model Checking 21
  - 2.6.1 Verification Conditions 21

2.6.2 Well-founded Relations and Rankings 22
2.6.3 Manna and Pnueli's System 23
2.6.4 Diagram-Based Verification 24
2.7 Trees, Games and Strategies 26

3 LTL Proof Structures **29**
3.1 Definition of LTL Proof Structures 30
3.1.1 Discussion of the Rules 34
3.1.2 The Split Condition (A-SPL) 35
3.1.3 Derived Rules 37
3.2 The Success Criterion 39
3.2.1 Successful Paths 39
3.2.2 A Tentative Success Criterion for Proof Structures . . . 40
3.2.3 Trails and Success for Proof Structures 43
3.3 A Rule for Proving Success 48
3.3.1 Rule $\mathsf{A}(\mathsf{F}, \bigvee \mathsf{F}\,\mathsf{G})$ 48
3.3.2 Rule $\mathsf{A}(\mathrm{S})$ 50
3.4 Some Examples 53
3.4.1 A Guarantee Property 53
3.4.2 A Safety Property 54
3.4.3 A Persistence Property 55

4 Soundness and Completeness via Games **59**
4.1 CTL* Games 61
4.1.1 Game Definition 61
4.1.2 Characterisation of CTL* satisfaction 63
4.2 Trails and Strategies 66
4.2.1 Generative Paths and Admissibility 66
4.2.2 Internal Strategies of Trails 67
4.2.3 Winning and Losing Strategies 69
4.2.4 Represented Strategies 70
4.2.5 Winningness and Admissibility 73
4.2.6 Admissibility vs. Success 74
4.3 Existence of a Proof Structure 76
4.4 Soundness and Completeness of Rule $\mathsf{A}(\mathrm{S})$ 79
4.5 Main Result 79

5 ELL and CTL* Proof Structures **81**
5.1 ELL Proof Structures 82
5.1.1 Some Remarks on the Rules 84
5.1.2 Derived Rules 85

5.2 Definition of ELL Success 86
5.3 A Proof Rule for ELL Success 88
5.3.1 Rule $\mathsf{E}(\bigwedge \mathsf{G}\,\mathsf{F})$ 88
5.3.2 Rule $\mathsf{E}(\mathrm{S})$ 90
5.4 Example 91
5.5 Soundness and Completeness 94
5.5.1 Admissible Trails and Winning Strategies 94
5.5.2 Existence of an Admissible ELL Proof Structure 96
5.5.3 Winningness and Successful Proof Structures 99
5.5.4 Soundness and Completeness of Rule $\mathsf{E}(\mathrm{S})$ 100
5.5.5 Main Result 100
5.6 A Proof System for Full CTL* 100
5.6.1 Soundness and Completeness for CTL* 102
5.7 Using Invariants in Proofs 102

6 Proving Success under Fairness 105
6.1 Expressing Fairness in CTL* 106
6.2 LTL Success under Fairness 108
6.2.1 Rule $\mathsf{A}(\mathsf{F}, \bigvee \mathsf{F}\,\mathsf{G})_{fair}$ 108
6.2.2 Rule $\mathsf{A}(\mathrm{S})_{fair}$ for LTL Success 110
6.3 ELL Success under Fairness 112
6.3.1 Rule $\mathsf{E}(\mathsf{F}\,\mathsf{G}, \bigwedge \mathsf{G}\,\mathsf{F})$ 115
6.3.2 Rules $\mathsf{E}(\mathsf{F}\,\mathsf{G}, \bigwedge \mathsf{G}\,\mathsf{F})_{wuf}$ and $\mathsf{E}(\mathsf{F}\,\mathsf{G}, \bigwedge \mathsf{G}\,\mathsf{F})_{fair}$ 120
6.3.3 Rules $\mathsf{E}(\mathrm{S})_{fair}$ and $\mathsf{E}(\mathrm{S})^{\top}_{wuf}$ for ELL Success 124

7 Application: The Bakery Protocol 129
7.1 Program Specification 129
7.2 Property Specification 132
7.3 Verification of Mutual Exclusion 132
7.3.1 A Generic Proof of Invariance 132
7.3.2 A Refined Style of Invariance Proofs 133
7.4 Verification of Accessibility 136
7.4.1 Proving Success for Π_{acc} 138
7.5 Verification of Unboundedness 141
7.5.1 Checking the Side Conditions for Π_{unb2} 141
7.5.2 Proving Success for Π_{unb1} and Π_{unb2} 143

8 Conclusions and Related Work 149
8.1 Summary and Discussion 149
8.2 Related Work 153
8.2.1 Finite-State Model Checking 153

8.2.2 Deductive and Semi-Algorithmic Methods 154
8.2.3 Model Checking Games 157
8.3 Directions for Future Work 159

Bibliography **161**

Curriculum Vitae **171**