

Table of contents

1	Introduction	1
1.1	Abstract data types, Proof techniques	1
1.2	Motivation	2
1.3	Organization of the book	3
1.4	Acknowledgements	3
2	State of the Art.....	5
2.1	Abstract specification and programming languages	5
2.1.1	The AFFIRM programming environment	6
2.1.2	The GYPSY programming environment	7
2.1.3	The Stanford Pascal Verifier	8
2.1.4	The IOTA programming environment	8
2.1.5	The Alphard programming language.....	9
2.1.6	Summary	9
2.2	Proof systems.....	10
2.2.1	The LCF proof system	10
2.2.2	The Boyer-Moore theorem prover	11
2.2.3	The Illinois theorem prover	12
2.2.4	Plaisted's theorem prover	13
2.2.5	The SPADE proof system.....	13
2.2.6	Final remarks	14
2.3	Conclusions	14
2.4	References	15
3	The Programming Language.....	18
3.1	General presentation	18
3.1.1	Overview	18
3.1.2	Characteristic properties	19
3.1.3	Notations	20
3.2	Types and operators	20
3.2.1	Objects and types.....	20
3.2.2	Operator specification.....	21
3.2.3	Operator chapter	24
3.3	Constructions and algorithms.....	26
3.3.1	Abstract context.....	26
3.3.2	Constructions	29
3.3.3	Algorithms	31
3.3.4	Algorithm chapter	38
3.4	Structures and modules.....	39
3.4.1	Concrete context.....	39

3.4.2	Structures	39
3.4.3	Modules	40
3.4.4	Module chapter	42
3.5	Development with ATES	43
3.5.1	Books.....	43
3.5.2	Chapters	44
3.5.3	Actions on a book	44
3.5.4	Debugging	46
3.6	Advanced features.....	47
3.6.1	Genericity	47
3.6.2	Special operators	49
4	The Applications within the ATES Project.....	51
4.1	Introduction.....	51
4.2	The first application	52
4.2.1	Problem description.....	52
4.2.2	Formulation	52
4.2.3	The finite element method: theoretical overview.....	54
4.2.4	The finite element method: implementation overview.....	59
4.2.5	The F.E.M. model	64
4.2.6	Results validation.....	65
4.3	The second application	66
4.3.1	3-D extension of the library	66
4.3.2	3-D mesh generation	66
4.3.3	The Delaunay triangulation.....	67
4.3.4	Boundary conformity problems	70
4.3.5	General chart.....	71
4.3.6	Some applications	75
4.4	Performance considerations.....	79
4.4.1	Performances and ATES system	79
4.4.2	IO aspect.....	80
4.4.3	Memory aspect.....	80
4.4.4	CPU Aspect.....	81
4.4.5	CPU: A performance test.....	81
4.5	References	85
5	The Specification and Proof Language	88
5.1	Basic mathematical elements for proof	88
5.1.1	The sets.....	88
5.1.2	Functions and constants	92
5.1.3	Expressions and predicates	96

5.2	Axioms	103
5.2.1	Definition.....	103
5.2.2	Syntax	103
5.2.3	Example	104
5.3	Types and operator specifications	104
5.3.1	Modeling types	105
5.3.2	Defining pre- and post-conditions for operators.....	108
5.3.3	Specifying secondary variables.....	110
5.3.4	Specifications of system-generated operators.....	112
5.4	Proof elements.....	118
5.4.1	Loops and invariants.....	118
5.4.2	Syntax	118
5.4.3	Concrete models.....	122
5.4.4	Abstraction functions	122
5.4.5	Representation functions	123
6	Proving the Correctness of ATEs Programs.....	126
6.1	Definition of the correctness	126
6.1.1	An operational semantics of ATEs operators.....	126
6.1.2	A first order predicate logic	129
6.1.3	The predicate transformer WP	133
6.2	The interactive proof environment	142
6.2.1	Elements required for proofs	143
6.2.2	Predicate transformation and interactivity	143
6.2.3	The proof system's user interface	144
6.3	Proving the verification conditions.....	154
6.3.1	Introduction	154
6.3.2	The simplification methods.....	154
6.3.3	Relations with theorem proving	173
6.4	Example: the 1D heat transfer problem	175
6.4.1	Reading the input.....	180
6.4.2	Solving the discrete mathematical problem.....	181
6.4.3	Write result on output.....	184
6.4.4	The data-structures and their models.....	184
6.4.5	The actual proof	192
6.5	Conclusions.....	195
6.6	References	197
7	Extending the Techniques to Parallel Programs.....	200
7.1	Formal synthesis and verification of concurrent programs.....	200
7.1.1	Introduction	200
7.1.2	Parallelism within the sequential framework.....	201

7.1.3	Formal tools for nondeterministic concurrency.....	207
7.1.4	Development of a data transfer protocol.....	215
7.2	Validation of the approach in the real-time area.....	229
7.2.1	Objective	229
7.2.2	Ada features.....	230
7.2.3	Specifications and proofs	232
7.2.4	Related works	233
7.2.5	A short example	234
7.2.6	Specification and proof with LOTOS.....	236
7.2.7	Conclusion.....	253
7.3	References	254
8	Implementation Issues.....	258
8.1	Generalities	258
8.1.1	Some data about the system.....	258
8.1.2	Overview of the system organization	259
8.2	The ATES compiler.....	261
8.2.1	Initialisation.....	261
8.2.2	The parser.....	262
8.2.3	Semantic analysis of operators	263
8.2.4	Semantic analysis of algorithms.....	264
8.2.5	Semantic analysis of modules	274
8.2.6	Code generation	276
8.2.7	Code compilation and execution.....	279
8.3	The ATES proof system.....	279
8.3.1	Semantic analysis of axiom chapters.....	280
8.3.2	Semantic analysis of specification chapters	282
8.3.3	Semantic analysis of proof chapters.....	283
8.4	The ATES correctness proof system.....	286
8.4.1	The simplifier.....	286
8.4.2	The data manager.....	291
8.4.3	The graphic proof interface	292
8.5	References	293
9	Conclusion	294
	Appendix A. Formal Specification of the 1D Heat Transfer Problem	296
	Appendix B. Grammar of the ATES Specification Language.....	311
	Appendix C. Grammar of the ATES Source Language.....	320