

Table of Contents

1	Introduction	1
2	Informal Introduction to Deva	13
2.1	An Algebraic Derivation	13
2.1.1	The Problem	13
2.1.2	The Structure of the Formalization	14
2.1.3	Preliminaries	16
2.1.4	Parametric Equality	17
2.1.5	Natural Numbers	23
2.1.6	Proof of the Binomial Formula	28
2.2	Elements of Proof Design	31
2.2.1	Transitive Calculations	33
2.2.2	Lemmas and Tactics	33
2.2.3	Local Scope	36
2.2.4	Composition of Inference Rules	38
2.2.5	Backward Direction	41
2.3	Further Constructs	42
3	Stepwise Definition of Deva	45
3.1	Two Examples	45
3.2	The Explicit Part: Kernel	45
3.2.1	Formation	47
3.2.2	Intended Meaning of the Constructs	47
3.2.3	Environments	48
3.2.4	Closed Texts and Closed Contexts	49
3.2.5	Reduction of Texts and Contexts	50
3.2.6	Conversion	52
3.2.7	Type Assignment of Texts	54
3.2.8	Auxiliary Predicates for Validity	56
3.2.9	Validity	57
3.3	The Explicit Part: Extensions	58
3.3.1	Product	58
3.3.2	Sum	60
3.3.3	Cut	62
3.3.4	Context Operations	64
3.4	The Explicit Part: Illustrations	67
3.5	The Implicit Part	72
3.5.1	Formation	72
3.5.2	Intended Meaning of the Constructs	73
3.5.3	Environments	74
3.5.4	Homomorphic Extensions	75
3.5.5	Closed Expressions	77
3.5.6	Extension of Reduction and Explicit Validity	77
3.5.7	Auxiliary Semantic Predicates for Implicit Validity	77

3.5.8 Explicitation	80
3.5.9 Explanation of Expressions	82
3.5.10 Implicit Validity	83
3.6 The Implicit Part: Illustrations	84
3.7 Mathematical Properties of Deva	86
3.7.1 Confluence	86
3.7.2 Closure Results	87
3.7.3 Strong Normalization	88
3.7.4 Decidability of Case-Free Validity	89
3.7.5 Recursive Characterization of Valid Normal Forms	90
3.7.6 Adequacy of Formalizations	90
3.8 Discussion	91
4 Formalization of Basic Theories	95
4.1 Overview	95
4.2 Logical Basis	97
4.2.1 Classical Many-Sorted Logic	97
4.2.2 Parametric Equality of Terms	102
4.2.3 Parametric Equality of Functions	104
4.3 Basic Theories of VDM	105
4.3.1 Natural Numbers	106
4.3.2 Finite Sets	107
4.3.3 Sequences	110
4.3.4 Tuples	113
4.3.5 Finite Maps	115
4.3.6 Simple Tactics	117
4.4 Basic Theories for Algorithm Calculation	118
4.4.1 Extensional Equality of Terms or Functions	119
4.4.2 Terms Involving Functions	121
4.4.3 Some Bits of Algebra	122
4.4.4 Induced Partial Ordering	125
5 Case Study on VDM-Style Developments	129
5.1 Overview	129
5.2 The Vienna Development Method	130
5.3 Formalization of VDM-Reification in Deva	130
5.3.1 Operations	131
5.3.2 Versions	132
5.3.3 Reification	134
5.4 The Human Leukocyte Antigen Case Study	137
5.4.1 Presentation	137
5.4.2 Development in VDM	138
5.5 Formalization of the HLA Development in Deva	142
5.5.1 HLA Primitives	143
5.5.2 HLA Abstract Specification	143
5.5.3 HLA Concrete Specification	147

5.5.4 Specification of the Retrieve Function	149
5.5.5 Proof of a Property of the Retrieve Function	151
5.5.6 HLA Development Construction	154
5.5.7 Proof of an Operation Reification	159
5.5.8 Proof of another Property of the Retrieve Function	163
5.6 Proof of Transitivity of Reification in Deva	168
5.6.1 Frequently Used Contexts	168
5.6.2 Simultaneous Induction on Version Triples	170
5.6.3 Global Proof Scheme	172
5.6.4 Verification of the Retrieve Condition	173
5.6.5 Transitivity of Operator Reification	174
5.6.6 Transitivity of the Reification Condition	176
5.6.7 Proof Assembly	179
5.7 Discussion	179
6 Case Study on Algorithm Calculation	181
6.1 Overview	181
6.2 Join Lists	182
6.3 Non-empty Join Lists	185
6.4 Some Theory of Join Lists	187
6.5 Some Theory of Non-Empty Join Lists	191
6.6 Segment Problems	192
6.7 Tree Evaluation Problems	199
6.8 Discussion	210
7 Conclusion	213
A Machine-level Definition of the Deva Kernel	221
B Index of Deva Constructs	225
C Crossreferences	227
C.1 Table of Deva Sections Defined in the Tutorial	227
C.2 Index of Variables Defined in the Tutorial	227
C.3 Table of Deva Sections Defined in the Case Studies	228
C.4 Index of Variables Defined in the Case Studies	233
D References	242