

Contents

1. Introduction	1
1.1 Symbolic computation	1
1.2 Verification	2
1.3 Higher order logic	3
1.4 Theorem proving vs. model checking	5
1.5 Automated vs. interactive theorem proving	6
1.6 The real numbers	8
1.7 Concluding remarks	9
2. Constructing the Real Numbers	13
2.1 Properties of the real numbers	13
2.2 Uniqueness of the real numbers	14
2.3 Constructing the real numbers	16
2.4 Positional expansions	17
2.5 Cantor's method	18
2.6 Dedekind's method	20
2.7 What choice?	21
2.8 Lemmas about nearly-multiplicative functions	24
2.9 Details of the construction	25
2.9.1 Equality and ordering	26
2.9.2 Injecting the naturals	27
2.9.3 Addition	27
2.9.4 Multiplication	28
2.9.5 Completeness	29
2.9.6 Multiplicative inverse	30
2.10 Adding negative numbers	31
2.11 Handling equivalence classes	33
2.11.1 Defining a quotient type	33
2.11.2 Lifting operations	34
2.11.3 Lifting theorems	35
2.12 Summary and related work	37

3. Formalized Analysis	39
3.1 The rigorization and formalization of analysis	39
3.2 Some general theories	40
3.2.1 Metric spaces and topologies	41
3.2.2 Convergence nets	43
3.3 Sequences and series	45
3.3.1 Sequences	49
3.3.2 Series	51
3.4 Limits, continuity and differentiation	53
3.4.1 Proof by bisection	54
3.4.2 Some elementary analysis	55
3.4.3 The Carathéodory derivative	57
3.5 Power series and the transcendental functions	59
3.6 Integration	61
3.6.1 The Newton integral	62
3.6.2 The Riemann integral	62
3.6.3 The Lebesgue integral	63
3.6.4 Other integrals	63
3.6.5 The Kurzweil-Henstock gauge integral	63
3.6.6 Formalization in HOL	65
3.7 Summary and related work	67
4. Explicit Calculations	69
4.1 The need for calculation	69
4.2 Calculation with natural numbers	69
4.3 Calculation with integers	73
4.4 Calculation with rationals	74
4.5 Calculation with reals	75
4.5.1 Integers	77
4.5.2 Negation	77
4.5.3 Absolute value	77
4.5.4 Addition	78
4.5.5 Subtraction	78
4.5.6 Multiplication by an integer	78
4.5.7 Division by an integer	79
4.5.8 Finite summations	79
4.5.9 Multiplicative inverse	79
4.5.10 Multiplication of real numbers	80
4.5.11 Transcendental functions	82
4.5.12 Comparisons	85
4.6 Summary and related work	86

5. A Decision Procedure for Real Algebra	87
5.1 History and theory	87
5.2 Real closed fields	89
5.3 Abstract description of the algorithm	90
5.3.1 Preliminary simplification	91
5.3.2 Reduction in context	91
5.3.3 Degree reduction	92
5.3.4 The main part of the algorithm	93
5.3.5 Reduction of formulas without an equation	94
5.3.6 Reduction of formulas with an equation	95
5.3.7 Reduction of intermediate formulas	96
5.3.8 Proof of termination	97
5.3.9 Comparison with Kreisel and Krivine	98
5.4 The HOL Implementation	99
5.4.1 Polynomial arithmetic	99
5.4.2 Encoding of logical properties	101
5.4.3 HOL versions of reduction theorems	102
5.4.4 Overall arrangement	106
5.5 Optimizing the linear case	106
5.5.1 Presburger arithmetic	108
5.5.2 The universal linear case	109
5.6 Results	110
5.7 Summary and related work	113
6. Computer Algebra Systems	115
6.1 Theorem provers vs. computer algebra systems	115
6.2 Finding and checking	118
6.2.1 Relevance to our topic	119
6.2.2 Relationship to NP problems	120
6.2.3 What must be internalized?	121
6.3 Combining systems	122
6.3.1 Trust	122
6.3.2 Implementation issues	123
6.4 Applications	124
6.4.1 Polynomial operations	125
6.4.2 Differentiation	127
6.4.3 Integration	129
6.4.4 Other examples	132
6.5 Summary and related work	132
7. Floating Point Verification	135
7.1 Motivation	135
7.1.1 Comprehensible specifications	135
7.1.2 Mathematical infrastructure	136
7.2 Floating point error analysis	137

7.3	Specifying floating point operations	138
7.3.1	Round to nearest	138
7.3.2	Bounded relative error	139
7.3.3	Error commensurate with likely input error	140
7.4	Idealized integer and floating point operations	142
7.5	A square root algorithm	143
7.6	A CORDIC natural logarithm algorithm	147
7.7	Summary and related work	153
8.	Conclusions	155
8.1	Mathematical contributions	155
8.2	The formalization of mathematics	155
8.3	The LCF approach to theorem proving	157
8.4	Computer algebra systems	158
8.5	Verification applications	158
8.6	Concluding remarks	159
A.	Logical foundations of HOL	161
B.	Recent developments	167