

Contents

Chapter 1. Gröbner Bases, an Introduction

Arjeh M. Cohen	1
1. Introduction.....	1
2. Monomials	4
3. The Buchberger Algorithm	7
4. Standard Monomials	15
5. Solving Polynomial Equations	17
6. Effectiveness of Polynomial Rings	23

Chapter 2. Symbolic Recipes for Polynomial System Solving

Laureano Gonzalez-Vega, Fabrice Rouillier, and Marie-Françoise Roy	34
1. Introduction.....	34
2. General Systems of Equations	35
2.1 Algebraic Preliminaries	35
2.2 First Recipes for Polynomial System Solving	40
3. Linear Algebra, Traces, and Polynomial Systems	46
3.1 Eigenvalues and Polynomial Systems	46
3.2 Counting Solutions and Removing Multiplicities	48
3.3 Rational Univariate Representation	51
4. As Many Equations as Variables	58
4.1 Generalities on Complete Intersection Polynomial Systems	58
4.2 Recipes for Polynomial System Solving When the Number of Equations Equals the Number of Unknowns.....	60
5. Gröbner Bases and Numerical Approximations.....	61

Chapter 3. Lattice Reduction

Frits Beukers	66
1. Introduction.....	66
2. Lattices.....	66
3. Lattice Reduction in Dimension 2	68
4. Lattice Reduction in Any Dimension	70
5. Implementations of the LLL-Algorithm	73
6. Small Linear Forms	75

Chapter 4. Factorisation of Polynomials

Frits Beukers	78
1. Introduction	78
2. Berlekamp's Algorithm	78
3. Additional Algorithms	81
4. Polynomials with Integer Coefficients	82
5. Factorisation of Polynomials with Integer Coefficients, I	84
6. Factorisation of Polynomials with Integer Coefficients, II	86
7. Factorisation in $K[X]$, K Algebraic Number Field	88

Chapter 5. Computations in Associative and Lie Algebras

Gábor Ivanyos and Lajos Rónyai	91
1. Introduction	91
2. Basic Definitions and Structure Theorems	91
3. Computing the Radical	97
4. Applications to Lie Algebras	105
5. Finding the Simple Components of Semisimple Algebras	108
6. Zero Divisors in Finite Algebras	112

Chapter 6. Symbolic Recipes for Real Solutions

Laureano Gonzalez-Vega, Fabrice Rouillier, Marie-Françoise Roy, and Guadalupe Trujillo	121
1. Introduction	121
2. Real Root Counting: The Univariate Case	122
2.1 Computing the Number of Real Roots	123
2.2 Sylvester Sequence	124
2.3 Sylvester-Habicht Sequence	128
2.4 Some Recipes for Counting Real Roots	133
3. Real Root Counting: The Multivariate Case	134
4. The Sign Determination Scheme	139
5. Real Algebraic Numbers and Thom Codes	142
6. Quantifier Elimination	145
7. Appendix: Properties of the Polynomials in the Sylvester-Habicht Sequence	149
7.1 Definition and the Structure Theorem	150
7.2 Proof of the Structure Theorem	154
7.3 Sylvester-Habicht Sequences and Cauchy Index	161

Chapter 7. Gröbner Bases and Integer Programming

Günter M. Ziegler	168
1. Introduction	168
2. What is Integer Programming?	168
3. A Buchberger Algorithm for Integer Programming	169

4. A Geometric Buchberger Algorithm	175
5. A Variant of the Buchberger Algorithm	177
6. Exercises	180

Chapter 8. Working with Finite Groups

Hans Cuypers, Leonard H. Soicher, and Hans Sterk	184
1. Introduction	184
2. Permutation Groups	185
2.1 The Setting	185
2.2 Computing Orbits and Stabilizers	187
2.3 Computing Bases and Strong Generating Sets	192
2.4 Generators for Some Subgroups	194
3. Coset Enumeration	197
3.1 Introduction	197
3.2 Todd-Coxeter Coset Enumeration	197

Chapter 9. Symbolic Analysis of Differential Equations

Marius van der Put	208
1. Introduction	208
2. The Equation $y' = f$ with $f \in C(x)$	208
2.1 The Algorithm	210
3. The Equation $y' = fy$ with $f \in C(x)^*$	212
4. Rational Solutions of an Equation of Order n	213
5. Some Differential Galois Theory	216
5.1 Picard-Vessiot Theory	218
6. Order Two Equations Over $C(x)$	222
7. The Local Differential Galois Group	225
8. The Equation $y'' = ry$ with $r \in C[x], r \neq 0$	229
9. The Equation $y'' = ry$ with $r \in C[x, x^{-1}]$	231

Chapter 10. Gröbner Bases for Codes

Mario de Boer and Ruud Pellikaan	237
1. Introduction	237
2. Basic Facts from Coding Theory	237
2.1 Hamming Distance	238
2.2 Linear Codes	238
2.3 Weight Distribution	239
2.4 Automorphisms and Isometries of Codes	239
3. Determining the Minimum Distance	240
3.1 Exhaustive Search	240
3.2 Linear Algebra	241
3.3 Finite Geometry	242
3.4 Arrangements of Hyperplanes	243
3.5 Algebra	245

4. Cyclic Codes	247
4.1 The Mattson-Solomon Polynomial	248
4.2 Codewords of Minimal Weight	250
5. Codes from Varieties	251
5.1 Order and Weight Functions	252
5.2 A Bound on the Minimum Distance	254

Chapter 11. Gröbner Bases for Decoding

Mario de Boer and Ruud Pellikaan	260
1. Introduction	260
2. Decoding	260
3. Decoding Cyclic Codes with Gröbner Bases	262
3.1 One-Step Decoding of Cyclic Codes	265
4. The Key Equation	267
4.1 The Algorithms of Euclid and Sugiyama	269
4.2 The Algorithm of Berlekamp-Massey	270
5. Gröbner Bases and Arbitrary Linear Codes	271

Project 1. Automatic Geometry Theorem Proving

Tomas Recio, Hans Sterk, and M. Pilar Vélez	276
1. Introduction	276
2. Approaches to Automatic Geometry Theorem Proving	277
3. Algebraic Geometry Formulation	277
4. Searching for Conditions	282
5. Searching for Extra Hypotheses	291

Project 2. The Birkhoff Interpolation Problem

Maria-Jose Gonzalez-Lopez and Laureano Gonzalez-Vega	297
1. Introduction	297
2. Poised Matrices	297
3. Examples	301
4. Conclusions	303

Project 3. The Inverse Kinematics Problem in Robotics

Maria-Jose Gonzalez-Lopez and Laureano Gonzalez-Vega	305
1. Introduction	305
2. The ROMIN Manipulator	305
3. The Elbow Manipulator	307

Project 4. Quaternion Algebras

Gábor Ivanyos and Lajos Rónyai	311
1. Introduction	311
2. Four Dimensional Simple Algebras	311
3. Quaternion Algebras and Quadratic Forms	312

Project 5. Explorations with the Icosahedral Group

Arjeh M. Cohen, Hans Cuyppers, Remko Riebeek 315

1. Introduction 315
2. Three-Dimensional Representations for $W(H_3)$ 316
3. Coset Enumeration 318
4. The Permutation Representation of W on the Cosets of I 318

Project 6. The Small Mathieu Groups

Hans Cuyppers, Leonard H. Soicher, and Hans Sterk 323

1. Introduction 323
2. The Affine Plane of Order 3 324
3. A 3 -($10, 4, 1$) Design and the Mathieu Group M_{10} 326
4. The Groups M_{11} and M_{12} 328
5. Two 2-Transitive Subgroups of M_{12} 329
6. Graphs Which Are Locally the Incidence Graph of the Biplane 332

Project 7: The Golay Codes

Mario de Boer and Ruud Pellikaan 338

1. Introduction 338
2. Minimal Weight Codewords of G_{11} 338
3. Decoding of G_{23} with Gröbner Bases 341
4. One-Step Decoding of G_{23} 343
5. The Key Equation for G_{23} 344
6. Exercises 346

Index 349