

# CONTENTS

Preface **xiii**

Current Textbooks in Algorithmic Algebra **xv**

## **0 Introduction 1**

- 0.1 FUNDAMENTAL PROBLEM OF ALGEBRA **2**
- 0.2 FUNDAMENTAL PROBLEM OF CLASSICAL ALGEBRAIC GEOMETRY **4**
- 0.3 FUNDAMENTAL PROBLEM OF IDEAL THEORY **6**
- 0.4 REPRESENTATION AND SIZE **9**
- 0.5 COMPUTATIONAL MODELS **10**
- 0.6 ASYMPTOTIC NOTATIONS **13**
- 0.7 COMPLEXITY OF MULTIPLICATION **15**
- 0.8 ON BIT VERSUS ALGEBRAIC COMPLEXITY **18**
- 0.9 MISCELLANY **20**
- 0.10 COMPUTER ALGEBRA SYSTEMS **26**

## **1 Arithmetic 27**

- 1.1 THE DISCRETE FOURIER TRANSFORM **28**
- 1.2 POLYNOMIAL MULTIPLICATION **32**
- 1.3 MODULAR FAST FOURIER TRANSFORM **34**
- 1.4 FAST INTEGER MULTIPLICATION **37**
- 1.5 MATRIX MULTIPLICATION **41**

## **2 The Greatest Common Denominator 43**

- 2.1 UNIQUE FACTORIZATION DOMAIN **44**
- 2.2 EUCLID'S ALGORITHM **47**
- 2.3 EUCLIDEAN RING **50**
- 2.4 THE HALF-GREATEST COMMON DENOMINATOR PROBLEM **54**
- 2.5 PROPERTIES OF THE NORM **57**

2.6 POLYNOMIAL HALF-GCD 61

APPENDIX A: Integer Half-GCD 67

### **3 Subresultants 77**

3.1 PRIMITIVE FACTORIZATION 78

3.2 PSEUDOREMAINDERS AND POLYNOMIAL REMAINDER SEQUENCE 82

3.3 DETERMINANTAL POLYNOMIALS 84

3.4 POLYNOMIAL PSEUDOQUOTIENT 87

3.5 THE SUBRESULTANT POLYNOMIAL REMAINDER SEQUENCE 89

3.6 SUBRESULTANTS 90

3.7 PSEUDOSUBRESULTANTS 92

3.8 SUBRESULTANT THEOREM 97

3.9 CORRECTNESS OF THE SUBRESULTANT POLYNOMIAL REMAINDER SEQUENCE ALGORITHM 101

### **4 Modular Techniques 104**

4.1 CHINESE REMAINDER THEOREM 104

4.2 EVALUATION AND INTERPOLATION 107

4.3 FINDING PRIME MODULI 111

4.4 LUCKY HOMOMORPHISMS FOR THE GCD 113

4.5 COEFFICIENT BOUNDS FOR FACTORS 116

4.6 A MODULAR GREATEST COMMON DENOMINATOR ALGORITHM 120

4.7 WHAT ELSE IN GCD COMPUTATION? 122

### **5 Fundamental Theorem of Algebra 124**

5.1 ELEMENTS OF FIELD THEORY 125

5.2 ORDERED RINGS 129

5.3 FORMALLY REAL RINGS 130

5.4 CONSTRUCTIBLE EXTENSIONS 132

5.5 REAL CLOSED FIELDS 135

5.6 FUNDAMENTAL THEOREM OF ALGEBRA 138

<b>6</b>	<b>Roots of Polynomials</b>	<b>141</b>
6.1	ELEMENTARY PROPERTIES OF POLYNOMIAL ROOTS	<b>142</b>
6.2	ROOT BOUNDS	<b>147</b>
6.3	ALGEBRAIC NUMBERS	<b>151</b>
6.4	RESULTANTS	<b>155</b>
6.5	SYMMETRIC FUNCTIONS	<b>161</b>
6.6	DISCRIMINANT	<b>167</b>
6.7	ROOT SEPARATION	<b>169</b>
6.8	A GENERALIZED HADAMARD BOUND	<b>173</b>
6.9	ISOLATING INTERVALS	<b>178</b>
6.10	ON NEWTON'S METHOD	<b>180</b>
6.11	GUARANTEED CONVERGENCE OF NEWTON ITERATION	<b>182</b>
<b>7</b>	<b>Sturm Theory</b>	<b>186</b>
7.1	STURM SEQUENCES FROM POLYNOMIAL REMAINDER SEQUENCES	<b>187</b>
7.2	A GENERALIZED STURM THEOREM	<b>190</b>
7.3	COROLLARIES AND APPLICATIONS	<b>195</b>
7.4	INTEGER AND COMPLEX ROOTS	<b>201</b>
7.5	THE ROUTH–HURWITZ THEOREM	<b>204</b>
7.6	SIGN ENCODING OF ALGEBRAIC NUMBERS: THOM'S LEMMA	<b>209</b>
7.7	PROBLEM OF RELATIVE SIGN CONDITIONS	<b>211</b>
7.8	THE BKR ALGORITHM	<b>214</b>
<b>8</b>	<b>Gaussian Lattice Reduction</b>	<b>219</b>
8.1	LATTICES	<b>219</b>
8.2	SHORTEST VECTORS IN PLANAR LATTICES	<b>224</b>
8.3	COHERENT REMAINDER SEQUENCES	<b>227</b>
<b>9</b>	<b>Lattice Reduction and Applications</b>	<b>234</b>
9.1	GRAM–SCHMIDT ORTHOGONALIZATION	<b>235</b>
9.2	MINKOWSKI'S CONVEX BODY THEOREM	<b>239</b>
9.3	WEAKLY REDUCED BASES	<b>242</b>
9.4	REDUCED BASES AND THE LLL ALGORITHM	<b>243</b>
9.5	SHORT VECTORS	<b>247</b>

9.6 FACTORIZATION VIA RECONSTRUCTION OF MINIMAL POLYNOMIALS 251

## 10 Linear Systems 258

- 10.1 SYLVESTER'S IDENTITY 259
- 10.2 FRACTION-FREE DETERMINANT COMPUTATION 262
- 10.3 MATRIX INVERSION 269
- 10.4 HERMITE NORMAL FORM 271
- 10.5 A MULTIPLE GCD BOUND AND ALGORITHM 275
- 10.6 HERMITE REDUCTION STEP 280
- 10.7 BACHEM-KANNAN ALGORITHM 286
- 10.8 SMITH NORMAL FORM 292
- 10.9 FURTHER APPLICATIONS 296

## 11 Elimination Theory 300

- 11.1 HILBERT BASIS THEOREM 301
  - 11.2 HILBERT NULLSTELLENSATZ 304
  - 11.3 SPECIALIZATIONS 308
  - 11.4 RESULTANT SYSTEMS 313
  - 11.5 SYLVESTER RESULTANT REVISITED 318
  - 11.6 INERTIAL IDEAL 321
  - 11.7 THE MACAULAY RESULTANT 327
  - 11.8  $U$ -RESULTANT 334
  - 11.9 GENERALIZED CHARACTERISTIC POLYNOMIAL 337
  - 11.10 GENERALIZED  $U$ -RESULTANT 342
  - 11.11 A MULTIVARIATE ROOT BOUND 350
- APPENDIX A: Power Series 355
- APPENDIX B: Counting Irreducible Polynomials 359

## 12 Gröbner Bases 363

- 12.1 ADMISSIBLE ORDERINGS 364
- 12.2 NORMAL FORM ALGORITHM 372
- 12.3 CHARACTERIZATIONS OF GRÖBNER BASES 378
- 12.4 BUCHBERGER'S ALGORITHM 382
- 12.5 UNIQUENESS 384
- 12.6 ELIMINATION PROPERTIES 386
- 12.7 COMPUTING IN QUOTIENT RINGS 391

## 12.8 SYZYGIES 393

**13 Bounds in Polynomial Ideal Theory 398**

13.1 SOME BOUNDS IN POLYNOMIAL IDEAL THEORY 399

13.2 THE HILBERT–SERRE THEOREM 401

13.3 HOMOGENEOUS SETS 407

13.4 CONE DECOMPOSITION 412

13.5 EXACT DECOMPOSITION OF  $\mathbb{N}\mathbb{F}(I)$  416

13.6 EXACT DECOMPOSITION OF IDEALS 423

13.7 BOUNDING THE MACAULAY CONSTANTS 424

13.8 TERM-REWRITING SYSTEMS 428

13.9 A QUADRATIC COUNTER 432

13.10 UNIQUENESS PROPERTY 436

13.11 LOWER BOUNDS 438

APPENDIX A: Properties of  $S_0$  442**14 Continued Fractions 446**

14.1 INTRODUCTION 447

14.2 EXTENDED NUMBERS 449

14.3 GENERAL TERMINOLOGY 451

14.4 ORDINARY CONTINUED FRACTIONS 455

14.5 CONTINUED FRACTIONS AS MÖBIUS TRANSFORMATIONS  
460

14.6 CONVERGENCE PROPERTIES 465

14.7 REAL MÖBIUS TRANSFORMATIONS 470

14.8 CONTINUED FRACTIONS OF ROOTS 474

14.9 ARITHMETIC OPERATIONS 478

References 485

Index 495

Index to Symbols 508