

Cambridge University Press
978-1-107-10963-6 - Solving Polynomial Equation Systems: Volume IV: Buchberger
Theory and Beyond
Teo Mora
Frontmatter
[More information](#)

SOLVING POLYNOMIAL EQUATION SYSTEMS

Volume IV: Buchberger Theory and Beyond

In this fourth and final volume the author extends Buchberger's algorithm in three different directions. First, he extends the theory to group rings and other Ore-like extensions, and provides an operative scheme that allows one to set a Buchberger theory over any effective unitary ring. Second, he covers similar extensions as tools for discussing parametric polynomial systems, the notion of SAGBI bases, Gröbner bases over invariant rings and Hironaka's theory. Finally, Mora shows how Hilbert's followers – notably Janet, Gunther and Macaulay – anticipated Buchberger's ideas and discusses the most promising recent alternatives by Gerdt (involutive bases) and Faugère (F_4 and F_5).

This comprehensive treatment in four volumes is a significant contribution to algorithmic commutative algebra that will be essential reading for algebraists and algebraic geometers.

Encyclopedia of Mathematics and Its Applications

This series is devoted to significant topics or themes that have wide application in mathematics or mathematical science and for which a detailed development of the abstract theory is less important than a thorough and concrete exploration of the implications and applications.

Books in the **Encyclopedia of Mathematics and Its Applications** cover their subjects comprehensively. Less important results may be summarized as exercises at the ends of chapters. For technicalities, readers can be referred to the bibliography, which is expected to be comprehensive. As a result, volumes are encyclopedic references or manageable guides to major subjects.

Cambridge University Press

978-1-107-10963-6 - Solving Polynomial Equation Systems: Volume IV: Buchberger
Theory and Beyond

Teo Mora

Frontmatter

[More information](#)

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing visit

www.cambridge.org/mathematics.

- 114 J. Beck *Combinatorial Games*
- 115 L. Barreira and Y. Pesin *Nonuniform Hyperbolicity*
- 116 D. Z. Arov and H. Dym *J-Contractive Matrix Valued Functions and Related Topics*
- 117 R. Glowinski, J.-L. Lions and J. He *Exact and Approximate Controllability for Distributed Parameter Systems*
- 118 A. A. Borovkov and K. A. Borovkov *Asymptotic Analysis of Random Walks*
- 119 M. Deza and M. Dutour Sikirić *Geometry of Chemical Graphs*
- 120 T. Nishiura *Absolute Measurable Spaces*
- 121 M. Prest *Purity, Spectra and Localisation*
- 122 S. Khrushchev *Orthogonal Polynomials and Continued Fractions*
- 123 H. Nagamochi and T. Ibaraki *Algorithmic Aspects of Graph Connectivity*
- 124 F. W. King *Hilbert Transforms I*
- 125 F. W. King *Hilbert Transforms II*
- 126 O. Calin and D.-C. Chang *Sub-Riemannian Geometry*
- 127 M. Grabisch *et al.* *Aggregation Functions*
- 128 L. W. Beineke and R. J. Wilson (eds.) with J. L. Gross and T. W. Tucker *Topics in Topological Graph Theory*
- 129 J. Berstel, D. Perrin and C. Reutenauer *Codes and Automata*
- 130 T. G. Faticoni *Modules over Endomorphism Rings*
- 131 H. Morimoto *Stochastic Control and Mathematical Modeling*
- 132 G. Schmidt *Relational Mathematics*
- 133 P. Kornerup and D. W. Matula *Finite Precision Number Systems and Arithmetic*
- 134 Y. Crama and P. L. Hammer (eds.) *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*
- 135 V. Berthé and M. Rigo (eds.) *Combinatorics, Automata and Number Theory*
- 136 A. Kristály, V. D. Rădulescu and C. Varga *Variational Principles in Mathematical Physics, Geometry, and Economics*
- 137 J. Berstel and C. Reutenauer *Noncommutative Rational Series with Applications*
- 138 B. Courcelle and J. Engelfriet *Graph Structure and Monadic Second-Order Logic*
- 139 M. Fiedler *Matrices and Graphs in Geometry*
- 140 N. Vakil *Real Analysis through Modern Infinitesimals*
- 141 R. B. Paris *Hadamard Expansions and Hyperasymptotic Evaluation*
- 142 Y. Crama and P. L. Hammer *Boolean Functions*
- 143 A. Arapostathis, V. S. Borkar and M. K. Ghosh *Ergodic Control of Diffusion Processes*
- 144 N. Caspard, B. Leclerc and B. Monjardet *Finite Ordered Sets*
- 145 D. Z. Arov and H. Dym *Bitangential Direct and Inverse Problems for Systems of Integral and Differential Equations*
- 146 G. Dassios *Ellipsoidal Harmonics*
- 147 L. W. Beineke and R. J. Wilson (eds.) with O. R. Oellermann *Topics in Structural Graph Theory*
- 148 L. Berlyand, A. G. Kolpakov and A. Novikov *Introduction to the Network Approximation Method for Materials Modeling*
- 149 M. Baake and U. Grimm *Aperiodic Order I: A Mathematical Invitation*
- 150 J. Borwein *et al.* *Lattice Sums Then and Now*
- 151 R. Schneider *Convex Bodies: The Brunn–Minkowski Theory (Second Edition)*
- 152 G. Da Prato and J. Zabczyk *Stochastic Equations in Infinite Dimensions (Second Edition)*
- 153 D. Hofmann, G. J. Seal and W. Tholen (eds.) *Monoidal Topology*
- 154 M. Cabrera García and Á. Rodríguez Palacios *Non-Associative Normed Algebras I: The Vidav–Palmer and Gelfand–Naimark Theorems*
- 155 C. F. Dunkl and Y. Xu *Orthogonal Polynomials of Several Variables (Second Edition)*
- 156 L. W. Beineke and R. J. Wilson (eds.) with B. Toft *Topics in Chromatic Graph Theory*
- 157 T. Mora *Solving Polynomial Equation Systems III: Algebraic Solving*
- 158 T. Mora *Solving Polynomial Equation Systems IV: Buchberger Theory and Beyond*
- 159 V. Berthé and M. Rigo (eds.) *Combinatorics, Words and Symbolic Dynamics*
- 160 B. Rubín *Introduction to Radon Transforms: With Elements of Fractional Calculus and Harmonic Analysis*
- 161 M. Ghergu and S. D. Taliaferro *Isolated Singularities in Partial Differential Inequalities*
- 162 G. Molica Bisci, V. Radulescu and R. Servadei *Variational Methods for Nonlocal Fractional Problems*
- 163 S. Wagon *The Banach–Tarski Paradox (Second Edition)*

Cambridge University Press

978-1-107-10963-6 - Solving Polynomial Equation Systems: Volume IV: Buchberger
Theory and Beyond

Teo Mora

Frontmatter

[More information](#)

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Solving Polynomial Equation Systems

Volume IV: Buchberger Theory and Beyond

TEO MORA

University of Genoa



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press
978-1-107-10963-6 - Solving Polynomial Equation Systems: Volume IV: Buchberger
Theory and Beyond
Teo Mora
Frontmatter
[More information](#)

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org

Information on this title: www.cambridge.org/9781107109636

© Cambridge University Press 2016

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2016

A catalog record for this publication is available from the British Library

ISBN – Volume I 978-0-521-81154-5 Hardback

ISBN – Volume II 978-0-521-81156-9 Hardback

ISBN – Volume III 978-0-521-81155-2 Hardback

ISBN – Volume IV 978-1-107-10963-6 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Contents

<i>Adieu</i>	<i>page ix</i>
PART SEVEN: Beyond	1
46 Zacharias	3
46.1 Buchberger–Zacharias Theory	5
46.2 Kandri-Rody–Kapur: Strong Gröbner Bases over a Euclidean Domain	27
46.3 Pan: Strong Gröbner Bases over a Principal Ideal Domain	31
46.4 Zacharias Rings	37
46.5 Möller : Gröbner Bases over Zacharias Rings	42
46.6 Möller: Gröbner Bases over a Principal Ideal Ring	48
46.7 Useless S-pairs and Gebauer–Möller Set in Principal Ideal Rings	50
46.8 Möller: Structural Theorem for Gröbner Bases over a Principal Ideal Ring	54
46.9 Lazard’s Structural Theorem over a Principal Ideal Ring	56
46.10 Ore Conditions	63
46.11 Ore Theory	68
46.12 Lazard’s Structural Theorem for Ore Extensions over a Principal Ideal Domain	83
46.13 Multivariate Ore Extensions	85
46.14 Ideal of Vanishing Polynomial	96
47 Bergman	100
47.1 Möller Left Lifting Theorem for Free Associative Algebras	102
47.2 Left Gröbner Bases for Free Associative Algebras	107
47.3 Möller’s Right Lifting Theorem and Right Gröbner Bases for Free Associative Algebras	115
47.4 Bilateral Gröbner Bases: The Lifting Theorem	117
47.5 Bilateral Gröbner Bases: Pritchard’s Module	121
47.6 Bilateral Gröbner Bases of an Ideal in a Free Monoid Rings over a Field	124

47.7	Pritchard's Procedure	144
47.8	La Scala–Levandovskyy: Letterplace Ideals	148
47.9	Gröbner Basis for Weaker Algebras	157
47.10	Green: Path Algebras	164
47.11	Reinert: Buchberger Theory on Function Rings	172
47.12	de Graaf–Wisliceny–Gerritzen: Gröbner Bases on Magma Algebras	184
48	Ufnarovski	191
48.1	Ufnarovski Graph	192
48.2	Ufnarovski: Finite-State Automata and Infinite Gröbner Basis Computation	198
48.3	2-Variable Graph	206
48.4	Shirayanagi: Word Tree	207
48.5	Anick's Resolution	212
48.6	Borges: Elimination Orderings and Symmetric Groups	217
48.7	Taxonomy of Term Orderings	221
48.8	Ideal Theoretical Operation	246
49	Weispfenning	256
49.1	Apel–Lassner: Lie Algebras and Buchberger Theory	258
49.2	Bergman: Diamond Lemma	261
49.3	Skew and Solvable Polynomial Rings	264
49.4	Kredel Conditions	268
49.5	Kandri-Rody–Weispfenning: Solvable Polynomial Rings	271
49.6	Twisted Polynomial Rings	278
49.7	Structural Theorem for Bilateral Ideals of a Twisted Polynomial Ring	284
49.8	Gateva's Monoid	288
49.9	Gateva: Noetherianity of Finitely Presented Algebras	291
49.10	Gateva: Binomial Skew Polynomial Rings	298
49.11	Weispfenning Rings	314
49.12	La Scala–Levandovskyy: Ore Extension of Multivariate Polynomial Rings	324
49.13	La Scala: Buchberger Theory for Partial Difference Ideals	332
50	Spear 2	335
50.1	Zacharias' Canonical Representation	336
50.2	Term Ordering	349
50.3	Pseudovaluations	351
50.4	Gröbner Bases and Buchberger Theory	359
50.5	Möller's Lifting Theorem	363
50.6	Spear's Theorem	371
50.7	Pseudovaluations (2)	377
50.8	Toward Buchberger's Algorithm	381
50.9	Buchberger's Algorithms	383
50.10	The Arithmetic of the Associated Graded Ring	386

<i>Contents</i>		vii
50.11	Noetherianity	394
50.12	Canonical Forms	397
50.13	Case Studies	399
51	Weispfenning II	423
51.1	Comprehensive Gröbner Bases	425
51.2	Montes' Algorithm	429
51.3	Canonical Comprehensive Gröbner Bases	436
51.4	Wibmer: Regular Functions	441
51.5	Kapur <i>et al.</i> : Branching via Solving Techniques	444
51.6	Montes–Wibmer: Canonical Gröbner Cover	446
51.7	Von Neumann Regular Rings	449
51.8	Gröbner Bases over Von Neumann Regular Rings	454
51.9	Comprehensiveness of Gröbner Bases over Von Neumann Regular Rings (1)	457
51.10	Suzuki–Sato: Alternative Comprehensive Gröbner Bases	459
51.11	Comprehensiveness of Gröbner Bases over Von Neumann Regular Rings (2)	465
52	Sweedler	468
52.1	Valuation Rings	471
52.2	Mosteing–Sweedler: Valuations and Filtrations	492
52.3	Mosteing–Sweedler: Characterizing Term Order Filtration	510
52.4	Subalgebra Bases	514
52.5	SAGBI Bases for Polynomial Invariants of Alternating Groups	519
52.6	Finiteness of SAGBI Bases	528
52.7	Göbel's Basis for Invariant Rings	531
52.8	Buchberger's Algorithm for Symideals	536
52.9	Aschenbrenner–Hillar: Buchberger Theory for Symmetric Ideals	542
52.10	Variations on SAGBI	552
53	Hironaka	565
53.1	A Theory of Normal Forms	567
53.2	Normal Forms and Standard Bases	572
53.3	The Zariskification of the Polynomial Ring	576
53.4	The Tangent Cone Algorithm	581
53.5	Standard Basis Algorithms	587
53.6	The Normal Form Algorithm	589
53.7	L -adic Valuation, Localization, Zariskification	592
53.8	Standard Bases in Local Rings	593
54	Hironaka II	597
54.1	Alonso–Luengo–Raimondo Model for Algebraic Power Series	597
54.2	Canonical Forms in the Ring of Algebraic Power Series	601
54.3	Standard Bases in the Ring of Algebraic Power Series	604
54.4	An Effective Version of the Weierstrass Preparation Theorem	611

54.5	Alonso–Castro–Hauser: An Effective Version of Hironaka’s Henselian Weierstrass Theorem	620
54.6	Branches of a Curve at a Singular Point	622
54.7	Toward Mac Millan’s Algorithm	626
54.8	Mac Millan’s Algorithm	630
55	Janet	633
55.1	Janet Decomposition	635
55.2	Riquier–Janet Completion	651
55.3	Degree-compatible Term Ordering and Convergency	658
55.4	Janet and Hilbert	661
55.5	Janet: Involutiveness	664
55.6	Term Orderings and the Borel Property in Riquier and His Followers	682
56	Macaulay V	691
56.1	Macaulay’s Formula	692
56.2	Hilbert Function	700
56.3	Sperner’s Proof of Macaulay’s Formula	702
56.4	Gunther: Borel Relation and Borel Invariance of Generic Forms	708
56.5	Gunther: Macaulay-like Formula for the Borel Set	716
56.6	Gunther’s Proof of Macaulay’s Formula	720
56.7	Gunther: Hilbert Function Computation	729
56.8	Gunther: Riquier–Janet Procedure	734
56.9	Bigatti–Hulett: Betti Numbers and Lex Segments	740
56.10	Marinari–Ramella: Revlex Segments	744
56.11	Cioffi–Roggero: J-marked Families	750
57	Gerdt and Faugère	757
57.1	Gerdt	758
57.2	Faugère	778
57.3	Mayr: Space-efficient Gröbner Basis Computation	796
57.4	Congedo: Buchberger–Wiesinger–Widi Groebnerian-Gaussian Bound	800
	<i>Bibliography</i>	803
	<i>Index</i>	813

Adieu

Churned in foam, that outer ocean lashed the clouds; and straight in my white wake,
 headlong dashed a shallop, three fixed specters leaning o'er its prow: three arrows
 poisoning.

And thus, pursuers and pursued flew on, over an endless sea.

H. Melville *Mardi: and A Voyage Thither*

He drew a deep breath. 'Well, I'm back,' he said.

In the original plan, the SPES survey was structured as a trilogy centered around the second volume, *Macaulay's Paradigm and Gröbner Technology*: after the first volume, *The Kronecker–Duval Philosophy*, formulated the task of 'solving' not as *producing programs which compute the roots* but as *producing techniques for computing with such roots*, the second volume introduced the Gröbnerian technologies needed for effectively and efficiently fulfilling this task. The third and last volume, according to this plan, would have consisted of a part¹ surveying all the recent approaches, mainly based on these techniques, which successfully completed the required task, and a final part covering extensions, applications, anticipations and alternatives to Gröbner bases.

This seventh and last part, *Beyond*, which grew to a gargantuan size and which is the present volume, covers the extensions of Buchberger's theory and algorithm in three different directions.

- Relaxing commutativity and allowing coefficients from a domain it is possible to export Buchberger theory over an effective ring monoid and to produce a Buchberger algorithm based on the Möller–Pritchard Lifting Theorem.

I cover the preliminary results by Zacharias, Kandri-Rody–Kapur, Pan and Möller on Buchberger theory over a domain; the extension from monoid rings toward weaker algebras (group rings, path algebras, magmas). In particular I cover the recent results by Birgit Reinert which cover function rings via saturation techniques.

I also cover the results of Ore on the construction of quotient fields over a non-commutative ring and on a non-commutative Euclidean algorithm, together with

¹ This part is the content of the third volume *Algebraic Solving*.

the related results by P.M. Cohn and a Buchberger theory for multivariate Ore extensions.

An intermezzo chapter covers applications of non-commutative Gröbner bases, combinatorial structures over monomial algebras and a (very preliminary) taxonomy of term orderings.

Next I cover the further relaxation, due to Weispfenning and his school, which dropped the requirement that variables and coefficients commute, thus allowing us to deal with Lie algebras, solvable polynomial rings, Ore extensions,...

Finally I propose an operative scheme – based on Spear’s theorem, Zacharias canonical representation and Möller–Pritchard Lifting Theory – which allows us to set a Buchberger theory over each effective associative ring.

- A chapter covers the tools for discussing parametric polynomial systems suggested by Weispfenning (comprehensive Gröbner bases) and settled by Montes and Wibmer with their GRÖBNER COVER package, and also Weispfenning’s extension of Buchberger theory toward Van Neumann regular rings.

A second chapter is devoted to the results put forward by Sweedler: his reconsideration of Buchberger theory in the setting of valuation rings and filtration and his notion of SAGBI bases. The chapter also covers related results extending/applying Buchberger theory towards invariant rings and symmetric ideals.

Finally, I cover Hironaka Theory of standard bases as a computational tool for local rings and algebraic power series; in connection I also discuss an old algorithm by Mac Millan which allows us to efficiently ‘compute’ the branches of a curve at a singular point.

- The last section merges pre- and post-Buchberger approaches.

I begin by discussing the anticipations of Buchberger theory that can be found in Riquier’s results and the related ‘solving’ techniques put forward by the followers of Hilbert as Janet, Gunther and Macaulay; the amazing aspect is that notions such as S-polynomials, generic initial ideals, Borel sets and even Galligo’s theorem had been published around 1890–1920.

What is more amazing is that the ideas of Riquier–Janet–Gunther (by Gerdt, under the name of involutive bases) and those of Macaulay (by Faugère with F_4 and F_5) have recently been reconsidered and are today the most efficient alternatives to Buchberger’s algorithm for computing Gröbner bases.

Bruno Buchberger presented his theory and algorithm of Gröbner bases to the computer algebra community at the EUROSAM’79 conference in Marseille in July 1979; the papers that applied it before that conference can be counted on the fingers of one hand.

I was present there and I am the person who introduced Buchberger theory to Italy; I have always been part of the large research activity that applied Buchberger theory to solving, to computerizing ideal theory and to extending it to weaker algebraic structures.

Consider SPES a diary of this 35-year-long journey and a map of the explored field.

Adieu

xi

This is the moment to express my thanks to all the friends who have accompanied me in this exciting voyage.

Allow me a last quotation of Macaulay²

I take this opportunity of thanking the Editors for their acceptance of this tract and the Syndics of the [Cambridge] University Press for publishing it

and, mainly, David Tranah for his constant support.

² Macaulay, F. S., *The Algebraic Theory of Modular Systems*, Cambridge University Press (1916), pp. vi.