Texts and Monographs in
Symbolic Computation

A Series of the
Research Institute for Symbolic Computation,
Johannes-Kepler-University, Linz, Austria

Edited by
B. Buchberger and G. E. Collins

D. Wang

Elimination Methods

Springer-Verlag Wien GmbH

Dr. Dongming Wang
Laboratoire d'Informatique de Paris 6
Université Pierre et Marie Curie, Paris, France

Originally published by Springer-Verlag Wien New York in 2001

Data conversion by Thomson Press (India) Ltd., New Delhi, India

Graphic design: Ecke Bonk
Printed on acid-free and chlorine-free bleached paper
SPIN 10637914

With 12 Figures

Library of Congress Cataloging-in-Publication Data

Wang, Dongming.
Elimination methods / D. Wang.
p. cm. — (Texts and monographs in symbolic computation, ISSN 0943-853X)
Includes bibliographical references and index.
ISBN 978-3-211-83241-7 ISBN 978-3-7091-6202-6 (eBook)
DOI 10.1007/978-3-7091-6202-6
1. Elimination. I. Title. II. Series.

QA192.W36 2000
512.9′434—dc21 00-035777

ISSN 0943-853X
ISBN 978-3-211-83241-7

To my parents and
to Xiaofan, Simon, and Louise

Preface

The development of polynomial-elimination techniques from classical theory to modern algorithms has undergone a tortuous and rugged path. This can be observed from B. L. van der Waerden's elimination of the "elimination theory" chapter from his classic *Modern Algebra* in later editions, A. Weil's hope to eliminate "from algebraic geometry the last traces of elimination theory," and S. Abhyankar's suggestion to "eliminate the eliminators of elimination theory." The renaissance and recognition of polynomial elimination owe much to the advent and advance of modern computing technology, based on which effective algorithms are implemented and applied to diverse problems in science and engineering. In the last decade, both theorists and practitioners have more and more realized the significance and power of elimination methods and their underlying theories. Active and extensive research has contributed a great deal of new developments on algorithms and software tools to the subject, that have been widely acknowledged. Their applications have taken place from pure and applied mathematics to geometric modeling and robotics, and to artificial neural networks.

This book provides a systematic and uniform treatment of elimination algorithms that compute various zero decompositions for systems of multivariate polynomials. The central concepts are triangular sets and systems of different kinds, in terms of which the decompositions are represented. The prerequisites for the concepts and algorithms are results from basic algebra and some knowledge of algorithmic mathematics. Some of the operations and results on multivariate polynomials which are used throughout the book are collected in the first chapter. Chapters 2 to 5 are devoted to the description of the algorithms of zero decomposition. We start by presenting algorithms that decompose arbitrary polynomial systems into triangular systems; the latter are not guaranteed to have zeros. These algorithms are modified in Chap. 3 by incorporating the projection process and GCD computation so that the computed triangular systems always have zeros. Then, we elaborate how to make use of polynomial factorization in order to compute triangular systems that are irreducible. The proposed algorithms and their underlying theories are based on the previous work of J. F. Ritt, W.-t. Wu, A. Seidenberg, and J. M. Thomas and its further development by the author. A brief review of some relevant algorithms including those based on resultants and Gröbner bases is given in Chap. 5. Elimination methods play a special role in constructive algebraic geometry and polynomial-ideal theory. Chapter 6 contains investigations on a few problems from these two areas. The book ends with an introduction to several selected applications of symbolic elimination methods.

Most of the algorithms presented in the book have been implemented by the author in the Maple system, and they are among the most efficient elimination algorithms available by this time. The algorithms are described formally so that the reader can easily work out his own implementation. Nevertheless, both theoretical complexity and practical implementation issues are not addressed in the book.

This book can be used as a textbook for a graduate course in elimination theory and methods. Some of the material was taught by the author at RISC-Linz, Johannes Kepler University a few times from 1989 to 1998.

I am very grateful to Professor Wen-tsün Wu who introduced me to the fascinating subject of polynomial elimination, taught me his method of characteristic sets, and has kept advising me for more than a decade. His work and thoughts have been so influential in my research that I have referred to them in most of my relevant publications.

I am greatly indebted to Professor Bruno Buchberger from whom I have learned so much beyond Gröbner bases. His generous support and help of numerous forms have made me easy at work and life for years.

Many colleagues and students have kindly helped me in different ways, like inviting me for a talk, a visit, or simply a dinner, being available to help when my languages run short, and giving me a hand when my computer gets stuck. It is impossible to mention all the names; I wish to thank all of them sincerely.

The members of the ATINF group led by Professor Ricardo Caferra at Laboratoire Leibniz, Institut d'Informatique et Mathématiques Appliquées de Grenoble deserve special thanks. They have created an ideal working environment, where I could enjoy thinking, writing, and programming. It is my pleasure to thank Mrs. Silvia Schilgerius and Mr. Thomas Redl at Springer-Verlag Wien, with whom I have worked for publishing this and two previous books.

Dongming Wang

Contents

List of symbols

$\triangleq$	"defined to be"
$\prec$, $\succ$	order for variables, terms, polynomials, and triangular sets
$\precsim$, $\succsim$, $\sim$	order for polynomials and triangular sets
$\backsim$	similarity of polynomials
$\sqrt{\ }$	radical (of an ideal)
$\Longleftrightarrow$	"if and only if"
$\rightsquigarrow$	"simplified to"
$\Rightarrow$, $\vee$, $\wedge$	logical "imply," "or," "and"

$\mathbf{A}^n_{\tilde{\boldsymbol{K}}}$	n-dimensional affine space over $\tilde{\boldsymbol{K}}$
$\mathbf{C}$	field of complex numbers
cls	class of a polynomial
coef	coefficient of a polynomial in a term
cont	content of a polynomial with respect to a variable
deg	degree of a polynomial in a variable
det	determinant of a square matrix
Dim	dimension of an algebraic variety or of a polynomial set or system
dim	dimension of a perfect triangular set or system
GB	reduced Gröbner basis of a polynomial set
gcd	greatest common divisor of a set of polynomials or of two polynomials with respect to a variable
Ideal	ideal generated by a set of polynomials
ini	initial of a polynomial; or the set of initials of the polynomials in a set
ITS	irreducible triangular series of a polynomial set or system
lc	leading coefficient of a polynomial (in a variable)
ldeg	leading degree of a polynomial
level	level of a polynomial set or system
lm	leading monomial of a polynomial
lt	leading term of a polynomial
lv	leading variable of a polynomial
$\boldsymbol{K}$	field of characteristic 0
$\tilde{\boldsymbol{K}}$	extension field of $\boldsymbol{K}$
$\tilde{\boldsymbol{K}}$-Zero	set of all zeros in $\tilde{\boldsymbol{K}}$ of a polynomial set or system
$\bar{\boldsymbol{K}}$	algebraic closure of $\boldsymbol{K}$
$\boldsymbol{K}(\theta)$	extension field obtained from $\boldsymbol{K}$ by adjoining θ

op	ith element of a tuple or an (ordered) set
$\mathbb{P}$	polynomial set (i.e., a finite set of nonzero polynomials)
$\mathbb{P}^{(i)}$	$\mathbb{P} \cap \boldsymbol{K}[x_1, \ldots, x_i]$
$\mathbb{P}^{[i]}$	$\mathbb{P} \setminus \mathbb{P}^{(i)}$
$\mathbb{P}^{\langle i \rangle}$	$\mathbb{P}^{(i)} \setminus \mathbb{P}^{(i-1)}$
$\mathbb{P}^{\langle \bar{x}, i \rangle}$	$\mathbb{P}\|_{x_1=\bar{x}_1, \ldots, x_i=\bar{x}_i}$
$[\mathbb{P}, \mathbb{Q}]$, $\mathfrak{P}$	polynomial system (i.e., a pair of polynomial sets)
$\mathfrak{P}^{(i)}$	$[\mathbb{P}^{(i)}, \mathbb{Q}^{(i)}]$ if $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$
$\mathfrak{P}^{\langle i \rangle}$	$[\mathbb{P}^{\langle i \rangle}, \mathbb{Q}^{\langle i \rangle}]$ if $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$
$\mathfrak{P}^{\langle \bar{x}, i \rangle}$	$[\mathbb{P}^{\langle \bar{x}, i \rangle}, \mathbb{Q}^{\langle \bar{x}, i \rangle}]$ if $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$
$\breve{\mathfrak{P}}$	$\mathbb{P} \cup \mathbb{Q}$ if $\mathfrak{P} = [\mathbb{P}, \mathbb{Q}]$
PB	prime basis of an irreducible triangular set
pp	primitive part of a polynomial with respect to a variable
pquo	pseudo-quotient of a polynomial with respect to a nonzero polynomial in a variable
prem	pseudo-remainder of a polynomial with respect to a nonzero polynomial (in a variable) or with respect to a triangular set; or set of pseudo-remainders of the polynomials in a set with respect to a polynomial or with respect to a triangular set
Q	field of rational numbers
R	field of real numbers
$\boldsymbol{R}$	ring
$\boldsymbol{R}[\boldsymbol{x}]$	ring of polynomials in $\boldsymbol{x}$ with coefficients in $\boldsymbol{R}$
Rad	radical of an ideal
red	reductum of a polynomial (with respect to a variable)
RegZero	set of regular zeros of a regular set, a triangular system, or a polynomial system
rem	remainder of a polynomial with respect to a polynomial set; or set of remainders of the polynomials in a set with respect to another polynomial set
res	resultant of two polynomials with respect to a variable or of a polynomial with respect to a triangular set
RS	regular series of a polynomial set or system
sat	saturation of a triangular set
sqfr	greatest squarefree divisor of a polynomial
SS	simple series of a polynomial set or system
$\mathbb{T}$	triangular set
$\mathbb{T}^{\{i\}}$	$[T_1, \ldots, T_i]$ if $\mathbb{T} = [T_1, \ldots, T_r]$
$[\mathbb{T}, \tilde{\mathbb{T}}]$, $\mathfrak{S}$	simple system
$[\mathbb{T}, \mathbb{U}]$, $\mathfrak{T}$	triangular system
tdeg	total degree of a polynomial
$\boldsymbol{u}$	$(u_1, \ldots, u_d)$, or $u_1, \ldots, u_d$
$\mathcal{V}$	algebraic variety
$\boldsymbol{x}$	$(x_1, \ldots, x_n)$, or $x_1, \ldots, x_n$
$\boldsymbol{x}^{\{i\}}$	$(x_1, \ldots, x_i)$, or $x_1, \ldots, x_i$
$\boldsymbol{\xi}$	$(\xi_1, \ldots, \xi_n)$, or $\xi_1, \ldots, \xi_n$, or $(\boldsymbol{u}, \eta_1, \ldots, \eta_r)$, or $\boldsymbol{u}, \eta_1, \ldots, \eta_r$

$\boldsymbol{\xi}^{\{i\}}$	$(\xi_1, \ldots, \xi_i)$, or $\xi_1, \ldots, \xi_i$, or $(\boldsymbol{u}, \eta_1, \ldots, \eta_i)$, or $\boldsymbol{u}, \eta_1, \ldots, \eta_i$
$\mathbf{Z}$	ring of integers
$\boldsymbol{z}$	$(\boldsymbol{u}, y_1, \ldots, y_r)$, or $\boldsymbol{u}, y_1, \ldots, y_r$
$\boldsymbol{z}^{\{i\}}$	$(\boldsymbol{u}, y_1, \ldots, y_i)$, or $\boldsymbol{u}, y_1, \ldots, y_i$
Zero	set of all zeros of a polynomial set or system