

Polynomials

*An Algorithmic
Approach*

Maurice Mignotte
Doru Ștefănescu



Springer

CENTRE FOR DISCRETE MATHEMATICS
AUCKLAND AOTEAROA
& THEORETICAL COMPUTER SCIENCE

0174.14
M644

Polynomials

An Algorithmic Approach



Maurice Mignotte

University L. Pasteur, Strasbourg, France

Doru Ștefănescu

University of Bucharest, Romania



E200000291



Springer



Maurice Mignotte
University L. Pasteur
UFR de Mathématique et d'informatique
7 Rue Descartes
67084 Strasbourg
France

Doru Stefanescu
University of Bucharest
P.O. Box 30-95
Bucharest 39
Romania

ISBN 981-4021-51-2

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on micro-films or in any other way, and storage in databanks or in any system now known or to be invented. Permission for use must always be obtained from the publisher in writing.

© Springer-Verlag Singapore Pte. Ltd. 1999
Printed in Singapore

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Camera-ready by author
SPIN 10707971 5 4 3 2 1 0

Polynomials

0174.14
M644

200000291

Polynomiasl

爱 护 图 书

人 人 有 责

广东图书馆设备用品公司

Springer

Singapore

Berlin

Heidelberg

New York

Barcelona

Budapest

Hong Kong

London

Milan

Paris

Tokyo

Introduction

I cannot do it without comp[ut]ers.

The Winter's Tale (Shakespeare)

The computational legacy of precomputer era includes only a few mathematical objects. Among them integers and polynomials hold a special position.

Many of our pencil and paper computations, but also those done by a pocket calculator or a computer, require polynomial operations. Multiplication of large integers, interpolation of functions, derivation and integration, matrix computations, integration of differential equations are all using polynomial computations.

The use of electronic computers has required a critical examination of computational methods designed during the evolution of various branches of mathematics. These studies proved that, for various reasons (as the extremely large running time or the impossibility of storage of too big data), some methods could not be effectively implemented. Hence, the necessity of designing alternative algorithms avoiding these implementation problems became more and more stringent. It stimulated researches on algorithmic procedures, leading to new results and the emergence of new fields.

A careful analysis of various methods of polynomial algebra proves that almost everything done in the past is useful for current computational purposes. Many algorithms developed during centuries of research can be easily implemented and lead to efficient procedures. However, some classical algorithms were proved to be very slow. Some of them were replaced by procedures that take up a much less amount of time or memory, and others are still waiting for convenient computational approaches.

The critical examination of the computational aspects of polynomials has led to the revival of some subjects and the development of new topics. The computation of the greatest common divisor, the estimation of various sizes associated with a polynomial, the factorization of polynomials with integer coefficients or with coefficients in a finite field, the fast Fourier transform and the polynomial interpolation are some of the topics intensively studied during the last decades. Several classic algorithms were improved and faster methods were designed.

In this textbook we will give a well-balanced presentation of classic procedures which are computationally relevant and some algorithms discovered during the last years. We left out on purpose several topics, for which an extensive literature is available, such as polynomials with real coefficients (P. Borwein, T. Erdélyi [15], M. Mignotte [92]) and Gröbner bases (T. Becker–V. Weispfenning [10], W. W. Adams–P. Loustau [1]).

The book is structured as follows. The first chapter discusses the construction and the representation of polynomials. We present the basics on polynomial operations and we describe several fundamental algorithms: the polynomial division, the greatest common divisor, polynomial roots, elimination theory, symmetric functions, interpolation, irreducibility tests.

The second chapter is devoted to computational aspects of the analytic theory of polynomials. We study the location of roots of univariate polynomials with complex coefficients and we establish inequalities on the length, height, norm, Bombieri's norm and measure of polynomial factors. These inequalities are crucial in polynomial factorization and root finding.

The third chapter focuses on polynomials with coefficients in a finite field. We cover cyclotomic polynomials, the fast Fourier transform, irreducible polynomials, polynomial roots and algorithms of factorization of univariate polynomials over finite fields developed by Berlekamp and Niederreiter.

The final chapter, devoted to factorization of polynomials with integer coefficients, presents the methods of Schubert–Kronecker, Berlekamp–Zassenhaus and Lenstra–Lenstra–Lovász.

The book is primarily aimed at graduate students. The prerequisites include standard definitions in set theory, usual fields (rational, real and complex numbers) and basic algebra (elementary results on groups, rings, fields and linear algebra). A rather important place is given to exercises, which are not always direct applications of the main results. Many of them complement the main text, helping the reader to check his understanding of key concepts and to put them into practice. Fully worked out examples, hints and references will ease the process of solving exercises. In addition, details concerning the implementation of algorithms as well as indicators of their efficiency are usually provided.

All results in the book are numbered according to chapter and section. Definitions and algorithms are not numbered, while examples and exercises are globally numbered. Throughout the algorithms the delimiters $\diamond\diamond$ mark a commentary.

The book is intended for use in a course on Polynomial Algebra; parts of it can also be used as a supplementary text for courses on Scientific Computing (sections 1.4, 1.5, 1.7, 2.2, 2.3, 2.4, 2.5, 2.7, 3.3, 3.6), Analysis of Algorithms (sections 1.1, 1.2, 1.4, 3.3, 3.7, 3.8, 3.9, 4.1, 4.2, 4.3), Computational Polynomial Factorization (sections 1.3, 1.8 and 2.6, chapters 3 and 4) and Computational Geometry of Polynomials (sections 1.1, 1.2, 1.3, 1.5 and 1.6, chapter 2).

We are grateful to several people for their help in the preparation of this book:

- To Attila Pethő (Debrecen), Mihai Cipu, Laurențiu Panaitopol (Bucharest), Douglas Bridges (Hamilton), Cristian Calude, Garry Tee (Auckland), Karl Svozil

(Vienna) for stimulating discussions on polynomials and computer algebra.

- To Cristian Calude for the invitation to publish this book in the DMTCS series at Springer Verlag, Singapore and for useful suggestions relative to this book.

- To Cătălina Ștefănescu who read and commented an earlier version of this text.

Parts of this book were taught by the authors at universities in Strasbourg, Bucharest, Montreal, Auckland, Abidjan, Niamey, Cagliari, Debrecen, Wuhan, Lanzho and Tienjin.

Maurice Mignotte, Doru Ștefănescu
Strasbourg, Bucharest, Săcele
July 1998

Springer Series in Discrete Mathematics and Theoretical Computer Science

Editors

Douglas Bridges
Department of Mathematics
University of Waikato
Private Bag 3105
Hamilton
New Zealand
e-mail: douglas@waikato.ac.nz

Cristian S. Calude
Department of Computer Science
The University of Auckland
Private Bag 92019
Auckland
New Zealand
e-mail: cristian@cs.auckland.ac.nz

Advisory Editorial Board

John Casti
Santa Fe Institute

R.L. Graham
AT&T Research
Murray Hill

Helmut Jürgensen
University of Western Ontario
University of Potsdam

Anil Nerode
Cornell University

Arto Salomaa
Turku University

Gregory J. Chaitin
IBM Research
Division

Joseph Goguen
Oxford University

Edsger W. Dijkstra
University of Texas at Austin

Juris Hartmanis
Cornell University

Grzegorz Rozenberg
Leiden University

Springer-Verlag Singapore's series in *Discrete Mathematics and Theoretical Computer Science* is produced in cooperation with the Centre for Discrete Mathematics and Theoretical Computer Science of the University of Auckland, New Zealand. This series brings to the research community information about the latest developments on the interface between mathematics and computing, especially in the areas of artificial intelligence, combinatorial optimization, computability and complexity, and theoretical computer vision. It focuses on research monographs and proceedings of workshops and conferences aimed at graduate students and professional researchers, and on textbooks primarily for the advanced undergraduate or lower graduate level.

For details of forthcoming titles, please contact the publisher at:

Springer-Verlag Singapore Pte. Ltd.
#04-01 Cencon I
1 Tannery Road
Singapore 347719
Tel: (65) 842 0112
Fax: (65) 842 0107
e-mail: gillian@springer.com.sg
<http://www.springer.com.sg>

Springer Series in

Discrete Mathematics and Theoretical Computer Science

D.S. Bridges, C.S. Calude, J. Gibbons, S. Reeves, I.H. Witten (Eds.), *Combinatorics, Complexity and Logic*. Proceedings, 1996. viii, 422 pages.

L. Groves, S. Reeves (Eds.), *Formal Methods Pacific '97*. Proceedings, 1997. Viii, 320 pages.

G.J. Chaitin, *The Limits of Mathematics: A Course on Information Theory and the Limits of Formal Reasoning*. 1998. xii, 148 pages.

C.S. Calude, J. Casti, M.J. Dinneen (Eds.), *Unconventional Models of Computation*. Proceedings, 1998. viii, 426 pages.

K. Svozil, *Quantum Logic*. 1998. xx, 214 pages.

J. Grundy, M. Schwenke, T. Vickers (Eds.), *International Refinement Workshop and Formal Methods Pacific '98*. Proceedings, 1998. viii, 381 pages

G. Păun (Ed.), *Computing with Bio-Molecules: Theory and Experiments*. 1998. x, 352 pages

C.S. Calude (Ed.), *People and Ideas in Theoretical Computer Science*. 1998.vii, 341 pages

C.S. Calude, M.J. Dinneen (Eds.), *Combinatorics, Computation and Logic'99*. Proceedings, 1999. viii, 370 pages

Contents

Introduction	v
1 An Introduction to Polynomials	1
1.1 Construction and Representation of Polynomials	1
1.1.1 Construction of polynomials	1
1.1.2 Representation of polynomials	4
1.2 Complexity and Cost	6
1.2.1 Complexity	6
1.2.2 Cost of polynomial operations	7
1.3 Polynomial Division	13
1.3.1 Divisibility	13
1.3.2 Unique factorization domains	14
1.3.3 The Euclidean division algorithm	16
1.3.4 Existence of gcd	17
1.3.5 Construction of gcd	18
1.3.6 Pseudo-division and polynomial remainder sequences . .	19
1.4 Polynomial Factorization	25
1.4.1 Polynomials over factorial rings	26
1.5 Polynomial Roots. Elimination. Resultants	29
1.5.1 Polynomial roots	29
1.5.2 Elimination theory. Resultants	33
1.5.3 The abridged method of Bézout	34
1.5.4 Jacobi's version	36
1.5.5 Cauchy's contribution	37
1.5.6 The companion matrix	39
1.6 Symmetric Functions	42
1.7 Polynomial Interpolation	48
1.7.1 Lagrange interpolation	49
1.7.2 Lagrange-Hermite interpolation	49
1.7.3 Newton interpolation	50
1.7.4 Taylor interpolation	51
1.7.5 Newton-Hermite interpolation	52
1.7.6 Finite differences	53
1.7.7 Chinese remainder theorem	54

1.8	Irreducibility Criteria	58
1.8.1	Irreducible polynomials in one variable	58
1.8.2	Irreducible polynomials in many variables	63
1.8.3	Generalized difference polynomials	66
2	Complex Polynomials	77
2.1	Polynomial Size	77
2.1.1	Norm	77
2.1.2	Measure	79
2.1.3	Length and height of a polynomial	83
2.1.4	Upper bounds for factors	85
2.2	Geometry of Polynomials	92
2.2.1	Location of polynomial roots	93
2.2.2	Apolar polynomials	95
2.3	Stable Polynomials	101
2.4	Polynomial Roots Inside the Unit Disk	108
2.5	Bounds for the Roots	113
2.5.1	Inclusion radii	113
2.5.2	Disks containing no roots	120
2.5.3	Disks containing at least one root	121
2.5.4	Disks containing at least a prescribed number of roots	123
2.6	Applications to Integer Polynomials	132
2.6.1	An irreducibility test	133
2.6.2	Primes and polynomial irreducibility	134
2.7	Separation of Roots	137
3	Polynomials with Coefficients in a Finite Field	141
3.1	Finite Fields	141
3.1.1	Construction of finite fields	142
3.1.2	Representation of elements of finite fields	148
3.2	Cyclotomic Polynomials	154
3.2.1	Definition of cyclotomic polynomials	154
3.2.2	Möbius inversion formula	156
3.2.3	Factorization of cyclotomic polynomials	157
3.3	Fast Fourier Transform	162
3.3.1	Discrete Fourier transform	162
3.3.2	Discrete fast Fourier transform	166
3.3.3	Fast multiplication of polynomials	169
3.4	Number of Irreducible Polynomials over a Finite Field	180
3.5	Construction of Irreducible Polynomials Over a Finite Field	186
3.5.1	Exponents of polynomials over a finite field	186
3.5.2	Irreducibility of binomials	192
3.5.3	Artin-Schreier polynomials	193
3.6	Roots of Polynomials Over Finite Fields	196
3.7	Squarefree Polynomials	200
3.7.1	Definition of squarefree polynomials	200

3.7.2	Factorization into a product of squarefree polynomials . . .	200
3.7.3	The number of squarefree polynomials	202
3.8	Berlekamp's Algorithm	204
3.8.1	Factorization of polynomials over finite fields	204
3.8.2	Polynomial factorization over \mathbb{F}_p	205
3.8.3	Polynomial factorization over \mathbb{F}_q	207
3.8.4	Description of the algorithm	211
3.8.5	Berlekamp's method over large fields	214
3.9	Niederreiter's Algorithm	221
3.9.1	Factorization of squarefree polynomials	222
3.9.2	Factorization of nonsquarefree polynomials	225
3.9.3	Factorization over \mathbb{F}_2	228
3.9.4	The refinement by Göttert	230
3.9.5	Hasse–Teichmüller derivatives method	233
4	Integer Polynomials	241
4.1	Kronecker's Factorization Method	241
4.1.1	Kronecker's algorithm	241
4.1.2	Kronecker–Hausmann algorithm	243
4.1.3	A bound for factors	248
4.2	The Berlekamp–Zassenhaus Algorithm	249
4.2.1	Modern methods of factorization in $\mathbb{Z}[X]$	250
4.2.2	Size of factors	251
4.2.3	Hensel's lemma	252
4.2.4	Reconstruction of factors over the integers	256
4.3	The LLL Factorization Algorithm	261
4.3.1	Reduced bases for lattices	261
4.3.2	Reduced lattices	262
4.3.3	Basis reduction algorithm	265
4.3.4	Polynomial factorization and lattices	271
4.3.5	The factorization algorithm	276
4.3.6	Cost of the algorithm	280
	Bibliography	285
	Notation	295
	List of Algorithms	299
	Name Index	301
	Subject Index	303

Chapter 1

An Introduction to Polynomials

The last thing one knows when writing a book is what to put first.

Pensées (Pascal)

In this chapter we construct the polynomials and we discuss their representation for computational purposes. Some basic concepts on algorithms and on polynomial operations are presented. We describe fundamental constructions and algorithms as polynomial division, the computation of the greatest common divisor, polynomial roots, resultant computations, symmetric functions, polynomial interpolation and irreducibility tests.

1.1 Construction and Representation of Polynomials

In this section we give a rigorous definition and we provide convenient representations of polynomials. As it will be seen the representation of polynomials for computational purposes corresponds to “classic” algebraic techniques. Both abstract and computational polynomial approaches use the same concepts and methods.

1.1.1 Construction of polynomials

Polynomials are defined as members of an overring of a base ring, called the coefficient ring. It is sufficient to define polynomials in one variable, because there exists an inductive procedure for several variables.

Definition: Let A be a ring and consider the set \mathcal{S} of sequences

$$\{a_0, a_1, \dots, a_i, \dots\}, \quad a_i \in A$$

such that all but a finite number of a_i are 0.

For $P, Q \in \mathcal{S}$,

$$P = \{a_0, a_1, \dots, a_i, \dots\},$$

$$Q = \{b_0, b_1, \dots, b_i, \dots\},$$

we define the addition

$$P + Q = \{a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots\}$$

and the multiplication

$$P \cdot Q = \{a_0b_0, a_0b_1 + a_1b_0, \dots, a_ib_0 + a_{i-1}b_1 + \dots + a_{i-s}b_s + \dots + a_0b_i, \dots\}.$$

The triplet $(\mathcal{S}, +, \cdot)$ is a ring. An element P in this ring is called a *polynomial in one variable* (or *indeterminate*) with *coefficients* in A .

The polynomial defined by the sequence

$$X = \{0, 1, 0, \dots, 0, \dots\}$$

is said to be a *variable* (or *indeterminate*) over A .

The ring of polynomials $(\mathcal{S}, +, \cdot)$ is denoted by $A[X]$.

Remark: Note that

$$X^n = \{\underbrace{0, \dots, 0}_{n \text{ times}}, 1, 0, \dots, 0, \dots\}.$$

Therefore

$$P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n.$$

Definition: Let $P = \{a_0, a_1, \dots\} \in A[X]$. If all $a_i = 0$, then $P = 0$ is the *null* polynomial. If $P \neq 0$, let $n \in \mathbb{N}$ be minimal such that $a_n \neq 0$. Then $n = \deg(P)$ is called the *degree*¹ of the polynomial P . The coefficient a_n is called the *leading coefficient* of P and the term a_nX^n is called the *leading term*. If the ring A has a unity and $a_n = 1$, then P is called a *monic polynomial*.

In what follows we will use the notation: $a_n = \text{lc}(P)$, $a_nX^n = \text{lt}(P)$.

Definition: Let $P \in A[X]$. The function \tilde{P} defined by

$$\tilde{P}(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n \in A \quad \text{for all } \alpha \in A,$$

is called the *polynomial function* associated with the polynomial P . Usually the polynomial function \tilde{P} is also denoted by P .

¹We use the convention $\deg(0) = -\infty$.

Remark: It may happen that two distinct polynomials from $A[X]$ have associated the same function on A . For example, if the ring A is a finite set $\{a_1, \dots, a_n\}$ and $P, Q \in A[X]$, with

$$P(X) = (X - a_1) \cdots (X - a_n), \quad Q(X) = 0,$$

then $P \neq Q$, but $\tilde{P}(a) = \tilde{Q}(a) = 0$ for all $a \in A$.

Definition: Let A be an integral domain, $P, Q \in A[X]$, $Q \neq 0$. The quotient P/Q is called a *rational function* in one variable over A . The set of all univariate rational functions over A is denoted by $A(X)$.

The integer

$$\deg(P/Q) = \deg(P) - \deg(Q)$$

is called the *degree of the rational function* P/Q .

Definition: If $B \supseteq A$ is an overring and $b \in B$, set $P(b) = a_0 + a_1b + \dots + a_nb^n$ and note that $P(b) \in B$. We say that $P(b)$ is the result of *substituting* b for X in the expression $P(X)$ of P . In particular $P = P(X)$ (we take $B = A[X]$). The mapping $P \mapsto P(b)$ establishes a ring homomorphism $A[X] \rightarrow B$.

We recall some basic properties of polynomials.

Lemma 1.1.1 *If $P, Q \in A[X]$, then*

$$\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\},$$

$$\deg(P \cdot Q) \leq \deg(P) + \deg(Q).$$

Proposition 1.1.2 *If A is a domain and P, Q are nonzero polynomials in $A[X]$, then*

$$\deg(P \cdot Q) = \deg(P) + \deg(Q).$$

Note that, using the convention that $-\infty + a = -\infty$ for all $a < \infty$, Proposition 1.1.2 is valid also if one of the polynomials is zero.

Remark: If A is a ring, the ring of polynomials in n indeterminates (variables) over A is recursively defined by

$$(1) \quad A[X_1, \dots, X_{n-1}, X_n] := A[X_1, \dots, X_{n-1}][X_n],$$

where $A[X_1, \dots, X_{n-1}]$ is the coefficient ring.

An element $P \in A[X_1, \dots, X_n]$ is a *polynomial in n variables* (indeterminates) with coefficients in the ring A . Such a polynomial P is also called a *multivariate polynomial*. If $n = 2$ it is called a *bivariate polynomial*.

1.1.2 Representation of polynomials

There exist many ways of representing a polynomial $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$, but the most natural is the *list representation*

$$P = (a_0, a_1, \dots, a_n),$$

where the entries are the coefficients of f . It corresponds to the original definition of the polynomial P as a sequence with only a finite number of nonzero terms.

A variant of the list representation is

$$P = (X, n, a_n, \dots, a_1, a_0),$$

where n is the degree of P and a_n, \dots, a_0 are the coefficients. In this representation the order of the coefficients is reversed.

Definition: A polynomial representation is called *sparse* if the null coefficients are not explicitly represented. It is called *dense* if all the coefficients are mentioned, including those equal to zero.

Remark: The coefficients of a polynomial lie in a base ring and must be recognized by the machine. If the coefficients are integers, they are represented in a convenient base B . Usually B is 2 or 10, but it may be larger if we want to represent bigger integers. The same problem may happen if we deal with a dense polynomial of a very large degree. The polynomial is then split into two (or more) parts, each of them represented by a list which is an entry of another list.

The sparse representation is particularly useful for multivariate polynomials. Such polynomials have very few nonzero coefficients and it is convenient to store only the exponents and the coefficients of the nonzero monomials.

A version of the sparse representation is the *polygonal representation*. It associates to the polynomial $P(X) = \sum_{i \in I} a_i X^i$ the couples (i, a_i) for which $a_i \neq 0$.

Then $P(X)$ is represented by the ordered list

$$P = (X, a_s, m_s, \dots, a_2, m_2, a_1, m_1),$$

where all the coefficients a_i are nonzero and the exponents m_i are in decreasing order $m_s > \dots > m_2 > m_1$. Note that $\deg(P) = m_s$.

The null polynomial 0 is considered to be the empty list.

Remark: The sparse representation corresponds to Newton's diagram² of P . Both dense and sparse representations belong to classical approaches of polynomials.

The sparse representation allows the storage of a polynomial with considerably less space than in the case of a dense representation.

²The Newton diagram and Newton polygon will be considered in subsection 1.8.3.