Polynomials

An Algorithmic Approach

Maurice Mignotte
Doru Ştefănescu

Springer

CENTRE FOR DISCRETE MATHEMATICS
AUCKLAND AOTEAROA
& THEORETICAL COMPUTER SCIENCE

Polynomials

An Algorithmic Approach

Maurice Mignotte
University L. Pasteur, Strasbourg, France

Doru Ştefănescu
University of Bucharest, Romania

Springer

CENTRE FOR DISCRETE MATHEMATICS & THEORETICAL COMPUTER SCIENCE
AUCKLAND AOTEAROA

Maurice Mignotte
University L. Pasteur
UFR de Mathematique 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

Printed in Singapore

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

Polynomials

Springer
Singapore
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Tokyo

Introduction

I cannot do it without comp[u]ters.

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. Loustaunau [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 primarly 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 delimitors ◇◇ 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 Pethö (Debrecen), Mihai Cipu, Laurenţiu 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 Ştefănescu 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 Ştefănescu
Strasbourg, Bucharest, Săcele
July 1998

Springer Series in

Discrete Mathematics and Theoretical Computer Science

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

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

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

such that all but a finite number of a_i are 0.
For $P, Q \in \mathcal{S}$,

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

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

we define the addition

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

and the multiplication

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

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

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

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

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

Therefore

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

Definition: Let $P = \{a_0, a_1, \ldots\} \in A[X]$. 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: $a_n = \mathrm{lc}(P)$, $a_nX^n = \mathrm{lt}(P)$.

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

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

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

[1] We 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 $\{a_1, \ldots, a_n\}$ 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 $\widetilde{P}(a) = \widetilde{Q}(a) = 0$ 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 $P(b) = a_0 + a_1 b + \ldots + a_n b^n$ 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 $P \longmapsto P(b)$ establishes a ring homomorphism $A[X] \longrightarrow B$.

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

$$A[X_1, \ldots, X_{n-1}, X_n] := A[X_1, \ldots, X_{n-1}][X_n], \tag{1}$$

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

An element $P \in A[X_1, \ldots, X_n]$ 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*

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

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

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

where n is the degree of P and $a_n, \ldots, a_0$ 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 explicitely 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

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

where all the coefficients a_i are nonzero and the exponents m_i are in decreasing order $m_s > \ldots > m_2 > m_1$. 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 diagram[2] 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.

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