
Abstract of PhD Thesis

Author: Alin BOSTAN
Title: Algorithmique efficace pour des opérations
de base en calcul formel
Language: English (with an introduction in French)
Supervisors: Marc GIUSTI
Bruno SALVY
Institute: École polytechnique, France
Date: 9 December 2003

Abstract

The subject of this thesis is the design and implementation of efficient algorithms for some basic operations in computer algebra, as well as their applications to related fields, such as cryptography and computational number theory.

The first part of the text is dedicated to basic algorithms on univariate polynomials. The tool which we use systematically is a constructive version of Tellegen's transposition principle, which makes it possible to obtain new algorithms for the problems of multipoint evaluation and interpolation (in various polynomial bases and for various families of evaluation points), as well as a theorem of equivalence between the complexities of these two problems.

The second part is devoted to fast computation with algebraic numbers. We begin by studying certain elementary operations, as the composed sum and the composed product and their generalization – the diamond product of Brawley and Carlitz. Their calculation rests on the use of the formal Newton operator and the algebraic duality, translated algorithmically by the use of transposition principle and baby step / giant step methods. The results are then generalized to the framework of zero-dimensional algebraic polynomial systems, for the computation of minimal polynomials in quotient algebras and that of rational parametrizations.

In the third and last part, we investigate the question of the efficient computation of a term in a linear recurrent sequence with polynomial coefficients. As an application, we obtain theoretical and practical improvements of a point-counting method used in hyperelliptic curve cryptography. Then, we propose an evaluation-interpolation type method for certain usual operations on linear differential operators with polynomial coefficients.

Table of Contents

I	INTRODUCTION	5
	1 Introduction	7
	1.1 Problématique et contributions : vue d'ensemble	8
	1.2 Paradigmes algorithmiques	13
	1.3 Détail des contributions	18
II	FUNDAMENTAL ALGORITHMS	43
	2 Multiplication of polynomials, matrices and differential operators	45
	2.1 Multiplication of univariate polynomials and power series	46
	2.2 Matrix multiplication	49
	2.3 Problems related to matrix multiplication	52
	2.4 Multiplication of linear differential operators	55
	3 Newton iteration	58
	3.1 Newton's algebraic iteration – generic algorithm	59
	3.2 Application to operations on power series	59
	3.3 Rational fractions and linear recurrences with constant coefficients	64
	3.4 Newton iteration for polynomial matrices	69
	4 Tellegen's principle into practice	74
	4.1 Introduction	75
	4.2 Definitions and notation	77
	4.3 Tellegen's principle	78
	4.4 Transposed polynomial multiplication	80
	4.5 Transposed polynomial division	84
	4.6 Transposed evaluation and interpolation	87
	4.7 Conclusion, future work	90
	5 Polynomial evaluation and interpolation on special sets of points	92
	5.1 Introduction	93
	5.2 The general case	97
	5.3 Transposed conversion algorithms	101
	5.4 Special case of an arithmetic progression	102
	5.5 The geometric progression case	108
	5.6 Fast conversions between monomial and Bernstein basis	113
	6 Equivalence between polynomial evaluation and interpolation	116
	6.1 Introduction	117
	6.2 Computational model, main result	119
	6.3 Program transposition	121
	6.4 From interpolation to evaluation	122
	6.5 From evaluation to interpolation	123

III	FAST ALGORITHMS FOR ALGEBRAIC NUMBERS	125
7	Fast computation with two algebraic numbers	126
7.1	Introduction	128
7.2	Fast conversion algorithms between polynomials and power sums	133
7.3	Two useful resultants that can be computed fast	138
7.4	Computing the diamond product	145
7.5	Applications and related questions	156
8	Fast algorithms for zero-dimensional polynomial systems	161
8.1	Introduction	163
8.2	On the dual of the quotient algebra	168
8.3	Computing minimal polynomials and rational parametrizations	171
8.4	Speeding up the power projection	176
8.5	Experimental results	180
8.6	Proof of the main result	182
IV	FAST ALGORITHMS FOR LINEAR DIFFERENTIAL AND DIFFERENCE OPERATORS	191
9	Linear recurrences with polynomial coefficients	193
9.1	Introduction	194
9.2	Shifting evaluation values	196
9.3	Computing one selected term of a linear sequence	200
9.4	The Cartier-Manin operator on hyperelliptic curves	204
9.5	Point-counting numerical example	208
9.6	Conclusion	209
10	Fast algorithms for linear differential operators	211
10.1	Introduction	212
10.2	From differential operators to power series solutions	213
10.3	Apparent singularities and bounds on the coefficients	214
10.4	From power series solution to differential operators	217
10.5	Application to lclm and tensor product	219
10.6	Conclusions	220
	References	225–243

Author's correspondence address Alin Bostan
Laboratoire STIX
École polytechnique
91128 Palaiseau, France

Alin.Bostan@stix.polytechnique.fr