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

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

Alin.Bostan@stix.polytechnique.fr