J. Symbolic Computation (1990) **9**, 225–228

Special Issue
Computational Algebraic Complexity
Editorial

ERICH KALTOFEN

Special Issue Guest Editor

BRUNO BUCHBERGER

Editor in Chief

1. Introductory Remarks

The articles contained in this issue of the journal deal in a broad sense with the subject of complexity theory in algebraic computation. The idea to attract some of the best research contributions in this area of symbolic computation to a special issue on this subject was suggested to the guest editor by Bruno Buchberger after a meeting in December 1986. We then began the search and solicitation of papers that we thought would be suitable for such an issue. In terms of subject selection we were mostly guided by Strassen's (1984) survey of this research area. We do not hesitate in saying that the final sequence of papers in this issue not only represents a surprising diversity of approaches and methods, but also contains—in our opinion—several of the most outstanding and significant contributions to the subject obtained in the past four years. Before we briefly discuss the individual contributions from our point of view, we like to express our gratitude to all who helped in the making of this issue, especially the authors who submitted their papers (despite an anticipated publication delay), and all referees, who must remain anonymous, for their constructive help in the selection process. We hope that with this issue the subject of computational algebraic complexity will stay a well represented topic in this journal.

2. Discussion of the Individual Contributions

The article by Bach and Shoup addresses a new question in the theory of randomized algorithms: is there a tradeoff between the number of random coin tosses needed and the probability of failure accomplishable, all while retaining polynomial expected running time? Bach and Shoup investigate the problem of factoring univariate polynomials over finite fields, which is one of the first problems in computer science on which the usefulness of randomization was demonstrated. They can show that the failure probability, that is the probability that their algorithm does not produce a full factorization of the input polynomial, can be kept exponential small in the number of random bits used. As a consequence of this result they can also obtain a more efficient deterministic method by

0747–7171/90/030225+04 $03.00/0

just trying all the combinations for the few random bits requested. In particular, they obtain a deterministic algorithm that runs in polynomial time as a function of the input size times the squareroot of the characteristic of the coefficient field.

The article by Canny introduces a new invariant to the theory of affine polynomial ideals over a field, the generalized characteristic polynomial, abbreviated by GCP. While Cayley's last century multi-polynomial resultant captures the solvability of a zero-dimensional projective system of polynomial equations, no such invariant can exist for affine systems. However, projectivization of an affine system brings with it the possibility that a solution at infinity is no more zero-dimensional. Under this condition, the u-resultant of the projective solution, for instance, collapses to zero, obliterating all information on the isolated affine solution points. Canny introduces the GCP, which is, following Macaulay, the quotient of two characteristic polynomials rather than the quotient of the two determinants that constitute the resultant. He shows that the trailing coefficient of the GCP enjoys similar properties as the resultant. E.g., in the u-resultant case it contains as its factors all isolated affine zeros.

The article by Coppersmith and Winograd constitutes, as the first paper committed, the crystallization point of this special issue. The paper is on asymptotically fast matrix multiplication, starting from two previous results. One is an idea by Strassen (1988) that allows the coercion of a trilinear aggregate that does not correspond to a matrix multiplication scheme to one that does. The other is a theorem by Salem and Spencer on the density of certain subsets of initial blocks of the integers with the property that no three integers in the subset form an arithmetic progression. Coppersmith and Winograd implicitly construct a scheme for matrix multiplication that at the time of the writing of this editorial still constitutes the frontier of the art of conceiving asymptotically fast methods. The reader will not only easily find the record breaking exponent of their algorithm in their paper, but also an open problem about the existence of a family of Abelian groups and subsets, which is seemingly unrelated to the matrix multiplication question, but whose resolution would imply the ultimate exponent 2.

The article by von zur Gathen improves on the functional polynomial decomposition algorithm published previously in this journal by Kozen and Landau (1989). Von zur Gathen's univariate solution is of sequential running time, as measured in coefficient field operations, a little bit above linear in the degree of the polynomial to be decomposed. Further results on a parallel version of the algorithm, a special bivariate factorization algorithm for so-called separated bivariate polynomials, and multivariate decomposition with the outer polynomial being univariate, complete the paper. This of von zur Gathen's work on the subject restricts itself to the so-called tame case, in which the degree of the outer function does not divide the characteristic of the coefficient field.

The article by the guest editor and Trager* focuses on a new representation of multivariate polynomials. The paper proposes to manipulate polynomials that are given by so-called black boxes, which are objects taking as input a value for each variable, and then producing the value of the polynomial they represent at the specified point. We show that within this representation the greatest common divisor and factorization problems are

*We wish to remark that the editorial process for this paper was handled entirely by the editor in chief.

solvable in randomized polynomial time in the usual parameters, at least for coefficients from an algebraic extension of the rationals. The output of our algorithms are black boxes for the goal polynomials, for instance, programs for all the irreducible normalized factors. These outputs can be easily converted to the standard sparse format using modern sparse interpolation techniques (see the paper by Zippel in this issue). They are also very compact and can be stored or transmitted easily. Lastly, we solve the somewhat more difficult problem of producing black box representations for the numerator and denominator of a multivariate rational function given by a black box.

The article by Rolletschek explores the efficiency of the Euclidean algorithm for those imaginary quadratic number rings that admit division with remainder. In an earlier paper published in this journal Rolletschek (1986) showed for the Gaussian integers that the most efficient way to obtain the greatest common divisor via a Euclidean remainder scheme, measured in terms of the number of division steps, is to use any of the norm-smallest remainder in every division. Here this optimality principle for the steepest descent scheme is extended to the discriminants -7 and -8 (the case of discriminant -3 having been settled previously by Lazard), while for -11 the principle is shown to be false: in fact, pairs of integers can be constructed in this number ring such that the steepest descent scheme requires arbitrarily more divisions than the optimal scheme does. Rolletschek introduces the use of finite state automata in the analysis of what regions of the complex plane the remainders of a standardized scheme can cycle through.

The article by Rónyai studies, from an algorithmic point of view, the Wedderburn-Artin structure theory of finite dimensional associative algebras over a finite field. The basic objects in this theory, such as the radical of such algebras, the decomposition of a semi-simple algebra into a direct product of simple ones, zero divisors, and the isomorphism from a simple algebra to a full matrix algebra, are all found in randomized polynomial time. Randomization is needed in all instances for solving arising polynomial factorization problems (see also the article by Bach and Shoup in this issue), that is, the algorithms constitute deterministic polynomial time reductions to that problem. An application of the results to a problem on permutation groups is also exhibited.

The article by Zippel deals with the problem of interpolating a sparse multivariate polynomial over fields of characteristic zero from its values. In his 1979 MIT Ph.D. thesis, Zippel originally conceived a method that used randomization and required, roughly speaking, cubic running time in the number of non-zero monomials present in the polynomial. Note that standard Lagrangian interpolation is exponential in the number of variables, independently on how many monomials there actually are in the polynomial. As it turns out, the special evaluations of Grigoryev and Karpinski (1987), used by Ben-Or and Tiwari (1988) in their sparse interpolation algorithm, are applicable to Zippel's approach as well, and result in a collection of surprisingly effective algorithms for sparse multivariate polynomial interpolation, which are presented here. Again estimating the efficiency coarsely, the best algorithms are now a bit above linear in the number of non-zero monomials present.

3. Present and Future Work

Clearly, this special issue cannot encompass all areas of vigorous and fruitful investiga-

tion on the subject of algebraic computational complexity. For instance, the areas of the Gröbner bases theory or the theory of real elementary geometry have been covered by other special issues of this journal (vol. 5, nrs. 1&2, vol. 6, nrs. 2&3), and lately complexity theoretic progress in these areas can be discerned (see, e.g., (Faugère et al. 1989) and (Renegar 1989)). We wish to point to some new work that advance several of the presented areas, and which we are aware of now. Shoup (1990) has been able to show that primitive elements in large finite fields can be selected using few random bits. Lakshman (1989) has made use of Canny's GCP to obtain complexity bounds for finding Gröbner bases for the radical of zero-dimensional affine ideals. Eberly (1989) in his recent Toronto Ph.D. thesis has developed the counterpart of Ronyai's theory to finite dimensional algebras over algebraic number fields. The sparse interpolation problem for arbitrary sample points has been investigated by Borodin and Tiwari (1989). Finally, the sparse interpolation methods in Zippel's article have been implemented by Wiley at Rensselaer Polytechnic Institute and demonstrated to be practical on polynomials with 100 monomials and more.

4. Literature Cited

Ben-Or, M. and Tiwari, P., "A deterministic algorithm for sparse multivariate polynomial interpolation," *Proc. 20th Annual ACM Symp. Theory Comp.*, pp. 301–309 (1988).

Borodin, A. and Tiwari, P., "On the decidability of sparse univariate polynomial interpolation," *Tech. Report* **RC 14923 (#66763)**, IBM Research Division, September 1989.

Eberly, W., "Computations for Algebras and Group Representations," *Tech. Report* **225**, Dept. Comput. Sci., Univ. Toronto, 1989.

Faugère, J. C., Gianni, P., Lazard, D., and Mora, T., "Efficient computation of zero-dimensional Gröbner bases by change of ordering," *Tech. Rep.* **89-52**, Univ. Paris 7, LITP, July 1989.

Grigoryev, D. Yu. and Karpinski, M., "The matching problem for bipartite graphs with polynomially bounded permanents is in NC," *Proc. 28th IEEE Symp. Foundations Comp. Sci.*, pp. 166-172 (1987).

Kozen, D. and Landau, S., "Polynomial decomposition algorithms," *J. Symbolic Comp.* **7/5**, pp. 445–456 (1989).

Lakshman, Y. N., "On the complexity of computing the Gröbner basis for the radical of a zero-dimensional ideal," *Proc. 22nd Annual ACM Symp. Theory Comp.*, to appear (1990).

Renegar, J., "On the computational complexity and geometry of the first-order theory of the reals: part I," *Tech. Report* **853**, Cornell University, School of Operations Research, Ithaca, N.Y., July 1989.

Rolletschek, H., "On the number of divisions of the Euclidean algorithm applied to Gaussian integers," *J. Symbolic Comp.* **2**, pp. 261–291 (1986).

Shoup, V., "Small degree primitive roots over finite fields," *Proc. 22nd Annual ACM Symp. Theory Comp.*, to appear (1990).

Strassen, V., "Algebraische Berechnungskomplexität," in *Anniversary of Oberwolfach 1984*, Perspectives in Mathematics; Birkhäuser Verlag, Basel, pp. 509–550, 1984. In German; updated English version to appear in the Handbook for Theoretical Computer Science.

Strassen, V., "The asymtotic spectrum of tensors," *J. reine angew. Mathematik* **384**, pp. 102–152 (1988).