

RESEARCH OVERVIEW OF AGNES SZANTO

The general objectives of my research program are to develop efficient algorithms for problems in algebra and in differential algebra, to analyze the computational complexity of the algorithms and to implement them. The scope of my research has expanded over the years. Initially I studied the structure of associative algebras and their applications to factoring polynomials and integers. As a Ph.D. student I turned my focus to the computational aspects of algebraic geometry and its application to the symbolic solution of polynomial and differential equation systems. As part of these investigations I became interested in subresultants, which is still one of my main research topics. My current research centers around symbolic-numeric algorithms for the solution of polynomial and differential systems. More precisely, I am looking at problems which are given with limited accuracy and which were traditionally called ill-conditioned, and find robust and efficient solutions using the integration of numerical and symbolic techniques.

Non-commutative algebra. In my undergraduate diploma, written under the direction of Lajos Rónyai, I addressed the problem of computing the decomposition of finite dimensional semisimple associative algebras over the function field $F_q(x)$ into simple algebras (Wedderburn decomposition). In [13] we gave a polynomial time reduction of the decomposition of algebras over $F_q(x_1, \dots, x_n)$ to the problem of factoring univariate polynomials over finite fields.

Furthermore, with Lajos Rónyai and Gábor Ivanyos, I investigated the effective isomorphism problem of simple algebras over number fields using results from class field theory, the theory of maximal orders, representation theory and quadratic forms. In [14] we constructed a polynomial time procedure to find zero divisors in rational quaternion algebras given a maximal order. This work required extending the lattice basis reduction of Lenstra, Lenstra and Lovász (cf. [18]) for the case of an indefinite symmetric bilinear form. Our algorithm produces a reduced basis with similar size properties as in the Euclidean case.

In a collaboration with Elizabeth L. Mansfield we studied non-commutative algebras defined by differential and difference operators: these are generalizations of the well known Ore-algebras, but here the algebra elements do not commute with each other neither with the base field. Our motivation was the application of these structures in the calculation of symmetries of discrete systems (cf. [12]). In [21] we could prove that differential-difference algebras provide a new instance of non-commutative graded rings which are effective Gröbner structures, and we gave an efficient algorithm to compute the Gröbner basis.

Symbolic Computation with Polynomial Systems. My Ph.D dissertation, written under the supervision of Dexter Kozen, and entitled “Computation with Polynomial Systems”, addresses the problem of computing a representation of algebraic sets such that set operations on algebraic sets are efficiently computable, and the representation is suitable for deriving improved time and space complexity bounds. In [24] and in [25] I have developed a fast parallel algorithm which finds a decomposition of the algebraic set into unmixed dimensional components, each component represented faithfully by characteristic sets. Moreover, for the first time I could prove that this algorithm has polynomial complexity bound in a randomized parallel computational model. This work has been cited by various authors, for example the algorithm has been extended to differential systems (cf. [11]), and been applied to compute with differential forms in algebraic geometry (cf. [1]).

Multivariate Subresultants. Multivariate subresultants were first introduced by Gonzalez-Vega (cf. [9, 10]), and later Chardin gave a construction using Koszul complexes which possessed

useful universal properties (cf. [3, 2]). Theoretical properties and applications of multivariate subresultants are active areas of research. A series of recent publications explored their application to solve polynomial systems, in the inverse parametrization problem of rational surfaces; their irreducibility and connection with residual resultants; the generalization of their universal properties to the affine well-constrained case; as well as generalizations of matrix constructions for subresultants.

My original interest in subresultants stems from the observation that, even in the univariate case, the most commonly used expressions for the common roots of a polynomial system derived from resultants are not optimal. In [26] I proved that subresultants give a more efficient alternative to solve over-constrained polynomial systems than resultant based methods. My other main contribution in the field was to give a matrix construction for subresultants based on Jouanolou's resultant matrices, which are significantly smaller than Chardin's subresultant matrices based on the classical Macaulay matrices, and to prove the equivalence of these formulations [25]. The proofs are highly non-trivial, relying on the understanding of the cohomology structure of some Koszul-Weymann complexes.

More recently, in a collaboration with Carlos D'Andrea, Hoon Hong and Teresa Krick, we were investigating rational expressions for subresultants as functions of the coordinates of the common roots of the given polynomials. We devised a simple and elegant technique based on linear algebra to prove some classical results of Sylvester [5], which technique was powerful enough to close some gaps in the works of Sylvester [6], as well as to give new generalizations to the multivariate case [7].

Symbolic-Numeric Solution of Polynomial Systems. The objective of the research is to develop the theory, algorithms, and software for solving systems of non-linear algebraic equations given with limited precision by using symbolic-numeric methods. In particular, the following types of systems are considered: 1. over-constrained systems of algebraic equations with inexact coefficients 2. algebraic equations which have multiple roots given with inexact coefficients. The research on this topic is sponsored by the CAREER Award from NSF.

In [23] we proposed an iterative method which computes for a given over-constrained system of equations the nearest system - measured as the 2-norm of the coefficient vector - which has at least k common roots and which is obtained via a perturbation of prescribed structure. In the univariate case we found close relationship between our problem and the optimization problem formulated by Karmarkar and Lakshman for the nearest GCD. In the multivariate case we could generalize the formulations of Karmarkar and Lakshman using Lagrange interpolation techniques to translate the original problem into an optimization problem on the k roots. Furthermore, we found that the above formulation can also be extended to systems with root multiplicities: the method presented in [22] computes the roots of the nearest system which has a given root multiplicity structure. Here we used multivariate Hermite interpolation techniques to translate the problem into an optimization problem on the roots. In both papers, after applying the Gauss-Newton method to these optimization problems, we gave explicitly the iteration function which computes the nearest system as well as the k common roots simultaneously. Moreover, based on an analogy to the classical Weierstrass iteration, we could simplify the Gauss-Newton iteration function via a basis transformation. Even though these new simplified iteration functions do not compute the 2-norm minimum, but we found and proved that its fixed points are the k roots of a system which was obtained via a local pointwise minimal perturbation of the input. Our simplified iteration function has improved complexity compared to iteration function computing

the minimal 2-norm optimum. We tested our methods on hundreds of random problem instances, and compared its performance to the Quadratic Interpolation and the Conjugate Gradient methods. Our numerical experiments show that our simplified iteration significantly speeds up the computation compared to other methods, and it did the best job decreasing the residual. Our findings were presented at the ISSAC 2004 conference as a poster, where it won the best poster award. Moreover, my student Mark Sciabica's Masters thesis is based on the above investigation.

In a collaboration with my student Itnuit Janovitz-Freireich, Bernard Mourrain and Lajos Rónyai we devised a new method which eliminates the near multiplicities of multivariate polynomial systems which have clusters of roots. We applied the classical Dickson's lemma to compute the "approximate radical" of a zero dimensional ideal I which has zero clusters: the approximate radical ideal has exactly one root in each cluster for sufficiently small clusters. Our method is "global" in the sense that it does not require any local approximation of the zero clusters, as opposed to most of the methods in the literature handling clusters of roots (cf. [20, 4, 8, 19]). In [16, 17] we reduce the problem to the computation of the numerical nullspace of the so called "matrix of traces", a matrix computable from the coefficients of the generating polynomials of I . We proved that if the size of the clusters is ε in the infinity-norm, then both the Gauss Elimination algorithm (cf. [16]) and the Singular Value Decomposition algorithm (cf. [17]) applied to the matrix of traces computes the approximate rank to a precision of ε^2 . Moreover, using the approximate nullspace of the matrix of traces we could compute the defining equations of an ideal, which we called the "approximate radical ideal", with the following properties: its roots are the arithmetic means of the clusters up to a precision of ε^2 . The bottleneck of the algorithm is the computation of the matrix of traces: in [15] we investigate how to compute the matrix of traces from the Bezout matrix of the input polynomials and their Jacobian in case the input is a well-constrained system. Furthermore, we are considering the computation of the radical ideal directly from the Bezout matrix, without the computation of the matrix of traces, which would give a new and more efficient alternative method both in the exact and in the approximate case.

Future Research. In the future, I plan to continue my investigations on symbolic-numeric algorithms for the solution of algebraic and differential equation systems. One of the topics I am presently interested in is certain representations of algebraic sets which are continuous in the coefficients of the input system as long as the basis of the factor algebra is unchanged. The ultimate goal of this approach would be the design of iterative methods for the solution of polynomial systems which behave robustly near systems with root multiplicities, and could be used as an alternative to Newton's method which fails at these singular systems. Since subresultants give criteria whether given sets of monomials generate the factor algebra, the above topic also leads to the need to a more general theory of subresultants, which extends the present notion to sets of monomials with arbitrary cardinality: I have some preliminary results in this direction.

I am also continuing my collaboration with C. D'Andrea, H. Hong and T. Krick to find a generalization of Sylvester's double sum formulae to multivariate subresultants, we already have some preliminary results for the special case of resultants.

Finally, our work on the computation of the approximate radical of ideals with clusters of roots rose some open questions, including: extension to higher dimensional ideals, more efficient ways to compute the matrix of traces, and finding ways to eliminate some of the roots of the system and thus lowering the size of the matrix of traces. I want to continue my collaboration with I. Janovitz-Freireich, B. Mourrain and L. Ronyai to try to answer some of these questions.

REFERENCES

- [1] Peter Burgisser and Peter Scheiblechner. Differential forms in computational algebraic geometry. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation (ISSAC '07)*, 2007.
- [2] Marc Chardin. Formules à la Macaulay pour les sous-résultants en plusieurs variables et application au d'un résultant réduit. *Comptes rendus de l'Académie des Sciences serie I-Mathématique*, 319(5):433–436, 1994.
- [3] Marc Chardin. Multivariate subresultants. *Journal of Pure and Applied Algebra*, 101:129–138, 1995.
- [4] Robert M. Corless, Patrizia M. Gianni, and Barry M. Trager. A reordered schur factorization method for zero-dimensional polynomial systems with multiple roots. In *Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, pages 133–140. ACM Press, 1997.
- [5] Carlos D'Andrea, Hoon Hong, Teresa Krick, and Agnes Szanto. An elementary proof of Sylvester's double sums for subresultants. *J. Symbolic Comput.*, 42(3):290–297, 2007.
- [6] Carlos D'Andrea, Hoon Hong, Teresa Krick, and Agnes Szanto. Sylvester's Double Sums: the general case. In *Proceedings of the MEGA 2007 (electronic)*, 2007.
- [7] Carlos D'Andrea, Teresa Krick, and Agnes Szanto. Multivariate subresultants in roots. *J. Algebra*, 302(1):16–36, 2006.
- [8] M. Giusti, G. Lecerf, B. Salvy, and J.-C. Yakoubsohn. On location and approximation of clusters of zeros of analytic functions. *Found. Comput. Math.*, 5(3):257–311, 2005.
- [9] Laureano González-Vega. Determinantal formulae for the solution set of zero-dimensional ideals. *Journal of Pure and Applied Algebra*, 76:57–80, 1991.
- [10] Laureano González-Vega. A subresultant theory for multivariate polynomials. In *ISSAC '91*, pages 79–85. ACM Press, 1991.
- [11] Evelyne Hubert. Factorization-free decomposition algorithms in differential algebra. *J. Symbolic Comput.*, 29(4-5):641–662, 2000. Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998).
- [12] P.E. Hydon. Symmetries and first integrals of ordinary difference equations. *Proceedings of the Royal Society of London*, (A 456):2835–2855, 2000.
- [13] Gábor Ivanyos, Lajos Rónyai, and Ágnes Szántó. Decomposition of algebras over $F_q(x_1, \dots, x_n)$. *Applicable Algebra in Engineering, Communication and Computing*, 5(2):71–90, 1994.
- [14] Gábor Ivanyos and Ágnes Szántó. Lattice basis reduction for indefinite forms and an application. *Discrete Mathematics*, 153:177–188, 1996.
- [15] Itnuit Janovitz-Freireich, Bernard Mourrain, Lajos Rónyai, and Ágnes Szántó. Computing Approximate Radicals using Bezoutians (extended abstract). In *Proceedings of the MEGA 2007 (electronic)*, 2007.
- [16] Itnuit Janovitz-Freireich, Lajos Rónyai, and Ágnes Szántó. Approximate radical of ideals with clusters of roots. In *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (ISSAC '06)*, pages 146–153, New York, NY, USA, 2006. ACM Press.
- [17] Itnuit Janovitz-Freireich, Lajos Rónyai, and Ágnes Szántó. Approximate radical for clusters: a global approach using Gaussian elimination or SVD. *Journal of Mathematics in Computer Science*, 1(2), 2007.
- [18] A. K. Lenstra, Jr. H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.
- [19] Anton Leykin, Jan Verschelde, and Ailing Zhao. Newton's method with deflation for isolated singularities of polynomial systems. *Theor. Comput. Sci.*, 359(1):111–122, 2006.
- [20] Dinesh Manocha and James Demmel. Algorithms for intersecting parametric and algebraic curves II: multiple intersections. *Graphical Models and Image Processing*, 57(2):81–100, 1995.
- [21] E. L. Mansfield and A. Szanto. Elimination theory for differential-difference polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC'03)*, pages 191–198, 2003.
- [22] S. Pope and A. Szanto. Nearest multivariate system with given root multiplicities. Submitted for publication.
- [23] Olivier Ruatta, Mark Sciabica, and Agnes Szanto. Over-constrained Weierstrass iteration and the nearest consistent system. Accepted in the Journal of Theoretical Computer Science.
- [24] Agnes Szanto. Complexity of the Wu-Ritt decomposition. In *Proceedings of PASCO'97*, pages 139–149. ACM Press, 1997.
- [25] Agnes Szanto. *Computation with polynomial systems*. PhD thesis, Cornell University, 1999.
- [26] Agnes Szanto (with an appendix by Marc Chardin). Solving over-determined systems by subresultant methods. Preliminary accepted in the Journal of Symbolic Computation.