Johannes Kepler University Linz

FWF-Doktoratskolleg (DK)

Computational Mathematics: Numerical Analysis and Symbolic Computation

October 2008 – September 2011

Speaker: Univ.-Prof. Dr. Peter Paule, Institute for Symbolic Computation (RISC), Johannes Kepler University, Altenberger Str. 69, 4040 Linz, Austria;
Phone: ++43-(0)732-2468-9921;
FAX: ++43-(0)732-2468-9930;
E-mail: Peter.Paule@risc.uni-linz.ac.at

Deputy Speaker: Univ.-Prof. Dr. Bert Jüttler, Institute for Applied Geometry, Johannes Kepler University, Altenberger Str. 69, 4040 Linz, Austria;
Phone: ++43-(0)732-2468-9178;
FAX: ++43-(0)732-2468-29162;
E-mail: Bert.Juettler@jku.at

Secretary of the Speaker: Marion Schimpl, Special Research Program (SFB) F013 "Numerical and Symbolic Scientific Computing", Johannes Kepler University, Altenberger Str. 69, 4040 Linz, Austria;
Phone: ++43-(0)732-2468-7174
FAX: ++43-(0)732-2468-7179;
E-mail: office@sfb013.uni-linz.ac.at

Linz, May 31, 2007 .....
(Prof. Dr. P. Paule, Speaker of the DK)

Linz, May 31, 2007 .....
(Prof. Dr. R. G. Ardelt, Rector, University of Linz)

Contents

1 General Information about the DK

1.1 Research Context

The proposed interdisciplinary graduate research program (DK) involves the Institutes of Applied Geometry (Geo), of Computational Mathematics (NuMa), of Industrial Mathematics (IndMath), and of Symbolic Computation (RISC) of the Johannes Kepler University, and the Johann Radon Institute for Computational and Applied Mathematics (RICAM) of the Austrian Academy of Sciences. The proposed DK will build on the expertise accumulated within the framework of the FWF Special Research Program SFB F013 "Numerical and Symbolic Scientific Computing", a research network consisting of exactly the same participating institutes.

The Special Research Program SFB F013 on "Numerical and Symbolic Scientific Computing" (`http://www.sfb013.uni-linz.ac.at`, speaker: Peter Paule) has started its work in April 1998. The overall and long-term scientific goal of the SFB was the design, verification, implementation, and analysis of numerical, symbolic, and geometrical methods for solving large-scale direct and inverse problems with constraints and their synergetical use in scientific computing for real life problems of high complexity. This included so-called field problems, usually described by partial differential equations (PDEs), and algebraic problems, e.g., involving constraints in algebraic formulation.

After each SFB funding period, 1998–2001 and 2001–2004, the SFB was evaluated by a team of external expert reviewers to decide about its continuation. As a result of the hearing from December 2003 the SFB was granted significantly increased funding for a third and last period of four years, from April 2004 until March 2008. In their report, the reviewers (from Canada, France, Germany, Holland, and Norway) especially appreciated the concept of combining symbolic and numeric computing. From the FWF-review-protocol: "Bringing these two worlds successfully together is probably the greatest achievement of this SFB. The reviewers stated that only few places exist worldwide, where comparable projects are tried, they were not aware of any other group that undertakes such an enterprise in this way. In this sense the SFB can be considered as unique." Concerning the educational aspect, the FWF-review-protocol says: "The reviewers especially appreciated the activities and the success of the SFB in educating young scientists: good training is provided for young people of different ages. The reviewers, however, felt that the share of PhD students could be increased against the number of PostDocs in the SFB." This resulted in an FWF funding of 17 PhD students and 5 PostDoc researchers for the last period of the SFB. As a consequence of the success of the SFB in this regard, the SFB participants unanimously decided to make an effort to establish a focused continuation of this kind of graduate education in the form of an FWF "Doktoratskolleg".

1.1.1 Overall scientific concept with short term and long term goals

In order to utilize the expertise accumulated during the period of the SFB, the long-term educational goal of the proposed DK is based on similar scientific grounds but stated slightly more generally as follows:

> Already for the first period, the overall goal of the DK program will be to provide intensive PhD training in two fundamental areas of computational mathematics: numerical analysis (in particular, of direct and inverse field problems) and symbolic

computation. This will be accomplished by course work that involves lectures from both areas and by interdisciplinary seminars. — The long-term goal is to establish a corresponding distinguished PhD Program at JKU which will attract young researchers from all over the world.

Such kind of DK education will stimulate numerous new avenues of research. For example: DK graduates will be able to develop new solvers to direct or inverse problems by combining numerical approaches with symbolic methods like Groebner bases; DK graduates will design new procedures for geometrical scientific computing by utilizing implementations of computer algebra algorithms for problems in algebraic geometry; DK graduates will use symbolic special function algorithms to speed-up hp finite element methods; DK graduates will use symbolic optimization techniques for constructing new algebraic multilevel preconditioners, etc. — It should be noted that first results in each of these directions have been already achieved within the SFB.

To achieve such results, interdisciplinary interaction is a necessary ingredient. Further details on this aspect are given in Section 1.1.3 in connection with the coherence of the DK.

1.1.2 Alphabetic list of participating researchers (Tab.1)

The following Table 1 presents an alphabetic list of participating DK researchers. *Note:* All researcher are male, so the corresponding column "sex" on the FWF form has been dropped.

Project leader	Research institution	Coordinates
Buchberger, Bruno Prof. Dr. Dr.hc.mult	J. Kepler University Research Institute for Symbolic Computation (RISC)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9921 fax: ++43-(0)732-2468-9930 Bruno.Buchberger@risc.uni-linz.ac.at
Jüttler, Bert Prof. Dr.	J. Kepler University Institute for Applied Geometry (Geo)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9178 fax: ++43-(0)732-2468-29162 bert.juettler@jku.at
Langer, Ulrich Prof. Dr.	J. Kepler University Institute of Computational Mathematics(NuMa)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9168 fax: ++43-(0)732-2468-9148 ulanger@numa.uni-linz.ac.at
Paule, Peter Prof. Dr.	J. Kepler University Research Institute for Symbolic Computation (RISC)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9921 fax: ++43-(0)732-2468-9930 Peter.Paule@risc.uni-linz.ac.at
Ramlau, Ronny Prof. Dr.	Austrian Academy of Sciences Johann Radon Institute for Computational and Applied Mathematics (RICAM)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-5232 fax: ++43-(0)732-2468-5412 ronny.ramlau@oeaw.ac.at

Project leader	Research institution	Coordinates
Schicho, Josef Prof. Dr.	Austrian Academy of Sciences Johann Radon Institute for Computational and Applied Mathematics (RICAM)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-5231 fax: ++43-(0)732-2468-5412 josef.schicho@oeaw.ac.at
Schreiner, Wolfgang Prof. Dr.	J. Kepler University Research Institute for Symbolic Computation (RISC)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9963 fax: ++43-(0)732-2468-9930 Wolfgang.Schreiner@risc.uni-linz.ac.at
Winkler, Franz Prof. Dr.	J. Kepler University Research Institute for Symbolic Computation (RISC)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9943 fax: ++43-(0)732-2468-9930 Franz.Winkler@risc.uni-linz.ac.at
Zulehner, Walter Prof. Dr.	J. Kepler University Institute of Computational Mathematics(NuMa)	Altenberger Str. 69, A-4040 Linz phone:++43-(0)732-2468-9171 fax: ++43-(0)732-2468-9148 zulehner@numa.uni-linz.ac.at

Table 1: Alphabetic list of participating researchers

1.1.3 Research areas, interdependencies and synergies (Tab.2)

Research areas in the first DK period. To achieve the overall goal, i.e., to provide intensive PhD training in numerical analysis and symbolic computation, 9 thesis research projects have been proposed. Here we give an informal summary of the PhD research areas that have been granted by the FWF; more detailed project descriptions can be found in Section 1.1.4.

DK1 has the objective of elaborating a comprehensive formal presentation of noncommutative Gröbner bases theory and algorithmics. On the object level, this is a contribution to recent computer algebra. On the meta level, this is a contribution to formal mathematical theory exploration based on automated reasoning. — Correspondingly, research for DK1 will be carried out both with groups in computer algebra (for example: the group of J.C. Faugère, Univ. Paris VI; the LinBox Project, M. Giesbrecht, U. of Waterloo, Canada, E. Kaltofen, NCSU, USA, et al.; the SINGULAR Project, G.M. Greuel et al., U. of Kaiserslautern, Germany; the group of M. Kreuzer, U. of Dortmund, Germany) and groups in automated reasoning (for example: Elsevier (Amsterdam), publisher of Journal of Symbolic Computation; the Mizar Group, U. of Byalystok, Poland; the group of J.L. Ruiz-Reina, U. of Sevilla, Spain).

DK3 proposes to investigate mathematical aspects of geometric computing, in particular geometric solvers for systems of polynomial equations. Interactions with other fields are e.g. real algebraic geometry and symbolic computation, computational geometry, and computer graphics. — Polynomial systems appear frequently in geometric computing with free–form curves and surfaces, e.g., for solving intersection problems. Geometric solvers, which rely on the Bernstein-Bézier representation, and their application in Geometric Computing, are an active research area. The proposer is in close contact with leading

experts: B. Mourrain (INRIA Sophia Antipolis), G. Elber (Technion Haifa), T. Dokken (SINTEF Oslo), L. Gonzalez-Vega (University of Cantabria, Santander), R. Farouki (University of California, Davis).

DK4 deals with boundary element based finite element methods and interface-concentrated finite element techniques allowing the efficient numerical treatment of boundary value problems which cannot be efficiently handled by standard finite element methods. It continues SFB F013 cooperations with the projects in symbolic computation (fundamental solutions, integration, special functions, symbolic construction of components of algebraic multigrid methods), with the integration of direct and inverse solution techniques and the work on geometrical problems. The proposer cooperates with T. Eibner (TU Chemnitz), B. Khoromskij (MPI Leipzig), J.M. Melenk (TU Vienna) and O. Steinbach (TU Graz) on the specific topics proposed in the DK4. Further international cooperations are listed below.

DK6 proposes to develop computer algebra tools for special function manipulation. Particular topics in connection with hp finite element methods concern the design of algorithms for multiple-integrals and of provers for special function inequalities. — Computer algebra for special function problems is a new and promising subarea of symbolic computation. In particular, an algorithmic/symbolic treatment of definite (multiple) integrals and of inequalities is only in a very early stage. The proposer's group is maintaining a regular scientific exchange with leading experts in the area, to name a few: the Algo-Group at INRIA Rocquencourt (F. Chyzak, F. Flajolet, B. Salvy), G.E. Andrews (PennState), T. Koornwinder (Amsterdam), M. Petkovšek (Ljubljana), and D. Zeilberger (Rutgers).

DK8 will study nonlinear regularization methods for the solution of linear ill-posed problems. Topics are: generalizations of two-step methods to other noise models, analysis of methods based on filter reduction, possible combination of data preprocessing and cg-method. — Although linear regularization methods have been studied for a long time, the investigation of nonlinear methods for the inversion of linear operator equations is a relatively new area. In particular the combination of data smoothing techniques and fast inversion methods has a huge potential for applications, in particular for the reconstruction of spatially inhomogeneous functions. The proposer is in close contact to some of the leading experts in the field, e.g. G. Teschke (Berlin), P. Maass (Bremen), S. Dahlke (Maarburg)

DK9 proposes to investigate new symbolic-numeric techniques for computing genus and parametrizing algebraic algebraic curves, based on topological methods. The relevant research areas are: symbolic-numeric algorithms, approximate algebraic computation, algorithmic algebraic geometry, geometric modeling, topology. — Numerical/approximate methods play an important role in computer algebra since approximately 15 years (compare, for instance, the percentage of symbolic/numeric contributions at leading periodic conferences such as ISSAC). Interactions between algebraic geometry and geometric modeling have been enforced recently by numerous joint meetings and joint projects, and in many of these, members of the proposer's group have been involved.

DK10 is devoted to the development of formally specified computer algebra software; e.g., tools to semi-automatically check whether computer algebra methods are adequately applied.

Sample software developed by other DK projects will be used to show the adequacy of the results. — In computer science, interest in using light-weight formal methods to find errors in software has surged in the last decade; corresponding specification languages and supporting tools for widely used programming languages have started to emerge and also to enter industrial practice in safety-critical areas (see e.g. the British VSR-net network for building up a Verified Software Repository). It is however still an open issue to adequately apply and adapt these results to widely used computer algebra languages; early work has e.g. been performed at St. Andrews (Ursula Martin and Steve Linton).

DK11 proposes the systematic investigation of applications of parametrizations of algebraic curves in computer aided geometric design, Diophantine analysis, and differential equations. Additionally, in close cooperation with DK 10, a redesign of the program system CASA is planned. — The investigation of algebraic curves is one of the oldest topics in mathematics and geometry. In recent decades, with the wide spread use of computer software, the computational aspects of this old and well-investigated theory have received new interest. Together with research groups in Madrid (J.R. Sendra), Santander (T. Recio, L. Gonzalez-Vega), University of Texas at Austin (C. Bajaj) and others we have been doing research in this area, and we intend to continue this work.

DK12 will develop efficient solvers for Karush-Kuhn-Tucker (KKT) systems. Topics range from the analysis of the behavior of symmetric indefinite block preconditioners to the construction of suitable preconditioners for interesting classes of discretized optimization problems in function spaces. — Because of the ubiquitous nature of saddle point problems (called KKT systems in the context of optimization problems) the development of efficient solvers for such systems has been of increasing interest for the last years. Although much has been achieved, many challenges remain, among them the development of new methods and the analysis of known and new methods, in particular, for solving large-scale systems from partial differential equations (PDEs) and PDE-constraint optimization, see a recent survey article by Benzi, Golub, Liesen. The proposer is jointly organizing a minisymposium on the subject with A. Wathen (Oxford) at the ICIAM (July 2007, Zurich), and has been invited to two further minisymposia, organized by Kanschat (Texas A&M University), M. Olshanskii (Moscow State University) and M. Sarkis (WPI/USA and IMPA/Brazil), X-Ch. Cai (University of Colorado at Boulder) on related topics at the same conference, an opportunity to strengthen the contact to leading experts in this field.

Interdependencies and synergies. Table 2 shows the assignment of the DK researchers to the DK research areas. *Note:* The field "Scientific discipline" is filled in according to the tables provided by "Statistik Austria" (ÖSTAT).

The overall goal of the DK program, namely, to provide intensive PhD training in both, numerical analysis *and* symbolic computation, can only be reached by ensuring strong inner coherence, i.e., by thesis research of strong interdisciplinary character. Table 2a gives a quick overview of the coherence and the interdisciplinary character of the DK. Namely, to each DK project proposed one finds particular other DK projects associated to it. These projects, listed in the right-most column, are those which have specific thematical connections to the given project, or with which specific kind of collaboration is desired.

Project leader	DK project part: no. and title	Scientific discipline
B. Buchberger	DK1: Formal Theory and Algorithmics of Noncommutative Gröbner Bases	computer algebra (1131)
B. Jüttler	DK3: Geometric Solvers for Polynomial Systems	geometry (1107)
U. Langer	DK4: Nonstandard Finite Element Solvers for Second-Order Elliptic Boundary Value Problems	numeric computation (1151)
P. Paule	DK6: Computer Algebra Tools for Special Functions in Numerical Analysis	computer algebra (1131)
R. Ramlau	DK8: Nonlinear Regularization Methods for the Solution of Linear Ill-posed Problems	numeric mathematics (1114)
J. Schicho	DK9: Symbolic-Numeric Techniques for Genus Computation and Parametrization	computer algebra (1131)
W. Schreiner	DK10: Formally Specified Computer Algebra Software	computer software (1105)
F. Winkler	DK11: Rational Parametric Algebraic Curves	computer algebra (1131)
W. Zulehner	DK12: Efficient Solvers for KKT Systems	numeric computation (1151)

Table 2: Assignment of the researchers to the research areas

Project leader	Affiliation	No. of proposed project	associated projects
B. Buchberger	RISC	DK1	DK6,10,11
B. Jüttler	Geo	DK3	DK4,9,12
U. Langer	NuMa	DK4	DK3,6,9,12
P. Paule	RISC	DK6	DK1,4,8,10
R. Ramlau	RICAM	DK8	DK6,9,12
J. Schicho	RICAM	DK9	DK3,4,8,10,11
W. Schreiner	RISC	DK10	DK1,6,9,11
F. Winkler	RISC	DK11	DK1,9,10
W. Zulehner	NuMa	DK12	DK3,4,8

Table 2a: DK Interdependencies

Besides presenting a quick overview of internal DK interaction, Table 2a also reflects various different kinds of proposed interdisciplinary research. For instance, there will be collaborations among DK scientists sharing the same scientific background (i.e., symbolic computation or numerical analysis) but being experts in different subareas of these fields. In addition, various projects will benefit by combining expertise in these areas with the geometry know-how of DK3. Another type of interaction concerns thesis projects that try to connect symbolic and numerical methods in a non-trivial way. All these kinds of interaction present an added value — in most significant form, the collaborations of the latter type. Joint SFB research already brought forward such type of joint research which proved to be extremely fruitful, both in the training of young PhD students as well as in the production of new scientific results. To accomplish such a goal, SFB PhD students — as well as SFB project leaders (!) — coming from different areas, first needed to learn how to communicate their mathematics to each other, before starting to think about combining methods from both sides. The proposed DK will build on this SFB experience.

1.1.4 DK PhD Thesis Topics

This subsection contains extended abstracts of the DK PhD Thesis Topics proposed. Each project description is structured as follows: (i) project number and name of the project leader, (ii) title of proposed thesis project, (iii) abstract (background information), (iv) current state of research (most relevant results in the field, recent work of the proposer), and (v) objectives and methods. The references given in the project descriptions refer to the lists of citations collected in Subsection 5.1 of the Appendix.

DK1 Bruno Buchberger: Formal Theory and Algorithmics of Noncommutative Gröbner Bases

Abstract

The goal of this thesis is a thorough presentation of the *theory and algorithmics of noncommutative Gröbner bases in a completely formal (logic) frame*, namely the Theorema version of predicate logic. In the first part of the thesis, using and extending the Theorema automated formal reasoning tools, the *theory should be formally verified* and, using the Theorema functor programming paradigm, *the algorithmics should be implemented in a generic, and also formally verified, way.* The subtle relation of (noncommutative) *Gröbner bases theory with linear algebra* based on the notion of generalized Sylvester matrix, which has significant potential for improving the algorithmics but was never carefully and completely studied theoretically, should be investigated in detail using the formal theory and the formal exploration tools provided in the first part of the thesis. If possible in the frame of just one thesis, one major application of noncommutative Gröbner bases theory, e.g. cryptography, should be explored and implemented. The thesis will also serve as an important input into a major research project "Math Journals as Active Reasoning Agents" by the same proposer in cooperation with a renowned international mathematics publishing company and will be carried out in close cooperation with the currently most active research groups in noncommutative Gröbner bases theory worldwide.

Current State of Research

Commutative Gröbner Bases Theory

Commutative Gröbner basis theory and its algorithmics were introduced, many years ago, in [5], [6], and, over the past decades, have found numerous applications both inside mathematics as well as in science and technology (for an overview, see for example, [7] and [47]). The latter textbook contains also a list of nearly all (approximately ten) currently available textbooks on Gröbner bases. A fairly complete, interactive bibliography on Gröbner bases was recently compiled, under the direction of B. Buchberger, by Alexander Zapletal in the frame of the "Special Semester on Gröbner Bases" at RICAM and RISC, Linz, (February - July 2006), see [48]. This bibliography contains, roughly, 1000 entries. The results of the eight workshops of the Special Semester will be published in, altogether, ten proceedings volumes which are currently composed and edited, by guest editors, under the overall scientific coordination of B. Buchberger. The importance and impact of Gröbner bases theory is also underlined by the fact that, a couple of years ago, an extra classification number, 13P10, has been introduced for Gröbner bases theory in the AMS classification index. Also, a search in the mathematical citation indices, e.g. the Research Index, http://citeseer.ist.psu.edu/, on Gröbner bases and related keywords yields several thousand entries. Since by the recent activities of the proposer the state of the art in Gröbner bases theory was, hence, intensively studied and documented, we do not give any more details here about the current state of Gröbner bases theory, algorithmics, and applications in general and concentrate here on the noncommutative case.

Noncommutative Gröbner Bases Theory

In this proposal, we choose one of the currently hot topics in the area of Gröbner bases theory, which is technically hard and, at the same time, promises to open - and is motivated by - quite a few new and deep applications, as has also been documented in the course of some of the workshops during the Special Semester on Gröbner Bases 2006.

The literature on noncommutative Gröbner bases, in the meantime, is also huge. A survey, together with a bibliography until 1998, was given in [14, 50]. Recent literature on the subject is compiled in the PhD thesis [34].

The theory of Gröbner bases in noncommutative polynomial domains, under a different name, can be traced to the seminal paper [2] (with early forerunners like [24]. In fact, in [2], the setting ("diamond lemma") is even more general and can be seen as a theoretical setting between the very general setting ("critical pairs" in [33]) of equational logic and rewriting on general term domains and the traditional setting ("S-polynomials") of commutative Gröbner bases theory introduced in [5, 6]. Explicitly, the theory and algorithmics of noncommutative Gröbner bases was introduced in close analogy to the commutative case and independently in a couple of papers, e.g. [31, 37, 1].

Applications of Noncommutative Gröbner Bases

The field of noncommutative Gröbner bases theory opens the horizon for a couple of fascinating new applications in established important areas as, for example: symbolics of combinatorial and special functions identities; symbolics of boundary value problems for differential equations; algebraic methods for cryptosystems and cryptoanalysis, see below. (We do not give more details on well-known applications in algebraic geometry, see for example [32], and for algebras in quantum physics, see for example [13])

Symbolics of Combinatorial and Special Functions Identities

Holonomic functions are solutions of systems of linear partial differential / difference equations of a certain particular form, called *holonomic systems.* Zeilberger [38] observed that many special functions are holonomic and he proposed the use of holonomic systems for the algorithmic treatment of special functions. Noncommutative Gröbner bases are applied in this context in the following way: The holonomic system defining a holonomic function gives rise to a finite set of differential/difference operators annihilating the function. These operators generate a left ideal in the (noncommutative) ring of operators, called the *annihilating ideal.* Proving identities about holonomic special functions typically requires the construction of an annihilating operator of a certain form, which can often be accomplished with a noncommutative Gröbner basis computation [39, 40, 41, 18]. For more details and a survey on this approach, see [16] and the references given there.

Symbolics of Boundary Value Problems for Differential Equations

One of the central themes of symbolic analysis is to develop computer algebra methods for dealing with differential equations. In this context, noncommutative Gröbner bases have proven

to be a powerful tool. For example, they can be used for the purpose of elimination in linear differential equation systems or evaluating parametrized integrals [41, 15, 17].

Differerential equations in applications often come along with boundary (in particular: initial) conditions. In symbolic computation, however, they are usually disregarded or accommodated in a post-processing step. Based on an operator approach first presented in [42], a symbolic method for computing the Green's operator for two-point boundary value problems with constant coefficients was given in [43, 44]. This approach has been extended to arbitrary linear ordinary differential equations in [45], including a method for factoring boundary value problems and Green's operators. The crucial step in determining Green's operators is the computation of normals forms using a suitable noncommutative Gröbner basis that reflects the essential interactions between basic operators.

Algebraic Methods for Cryptosystems and Cryptoanalysis

Public key cryptography [20] relies on the notion of (trapdoor) *one-way* function. Intuitively, such a function is easy (polynomial-time) to compute, but difficult (at best sub-exponential) to invert. One way functions themselves are constructed from *hard* problems (roughly speaking, problems for which no polynomial-time algorithm is known).

Thus, one of the main issues in public key cryptography is to identify hard problems, and propose new schemes that are not based on number theory (because the latter are not safe from a theoretical breakthrough). Following this line of research, cryptographic schemes using algebraic polynomials have been proposed. This area of cryptography is called *Multivariate Public-Key Cryptography*. Schemes in this approach are divided in two distinct families : "C*–like" schemes [21, 29] that are based on the hard problem of solving algebraic systems over a finite fields; and "Poly-Cracker"–like schemes [19] which are based on the difficulty of the ideal membership problem.

Recently, Ackermann-Kreuzer and Rai proposed several new schemes in this last family, [19, 49]. These new cryptosystems intensively use the theory of noncommutative Gröbner bases. Also, in order to evaluate the security of these new proposed schemes, strong and efficient cryptoanalytic methods – supported by noncommutative Gröbner bases theory – have to be developed. In a more constructive aspect, it seems natural to also investigate noncommutative versions of "C*–like" schemes. Surprisingly enough, this line of research has not been yet investigated. We believe that the real feasibility of such a variant deserves investigation.

Implementations of Noncommutative Gröbner Bases Theory

In order to put Gröbner bases theory on noncommutative (and other) polynomial domains into practice, one has to implement algorithms for constructing Gröbner bases as well as the algorithms that solve the fundamental problems in the ideal theory of the domains by reduction to Gröbner bases computations.

A couple of implementations of (part of) the algorithmics noncommutative Gröbner bases exist in current computer algebra systems like, for example, Singular, see [23]. For a complete list of available implementations, together with a comparison of available features, see the systems bibliogrpahy [35], which was compiled by V. Levandovsky in the frame of the Special Semester on Gröbner bases 2006 directed by B. Buchberger. From the comparison one sees that each of

the implementations has its pros and cons. However, none of them is generic in the sense that it can be easily adjusted to a variety of domains and non of them is formally verified.

In the proposer's Theorema Working Group we have build up a completely formal frame – the Theorema system – for the computer-supported build-up and verification of mathematical theories, including algorithms and their applications, see for example [3], [4]. The Theorema framework will be used (and extended) for the research work in this thesis.

Objectives and Methods

Research Objectives and Method of the Thesis

The objective of this thesis is a presentation of current noncommutative Gröbner bases theory and algorithmics with the following points of emphasis:

- The presentation of the theory should be *formal*.
- The algorithmics should be implemented *generically*.
- New research should be done on the subtle question of the relationship between *Gröbner bases and linear algebra* (based on the view of "generalized Sylvester matrices").
- In the ideal case, also on topical *application* should be included.

By a *formal* presentation we mean a presentation that is the result of formalizing the entire theory and its algorithmics in the frame of a formal logic language (for which we propose the Theorema version of predicate logic) and of proving all lemmas and theorems and verifying all algorithms by formal (partly automated) reasoners. Some of these reasoners (for example, a general predicate logic prover, various equality reasoners, various induction provers, a set theory prover, an algorithm synthesizer, and an algorithm verifier) are already available in Theorema, some others will have to be developed (and proved correct by the meta-proving mechanism of Theorema) in the course of the thesis. (The aspect of proving reasoners correct is subtle, see [9] and [10].

By a *generic* implementation we mean an implementation in which the algorithms have domain parameters whose instantiation by concrete domains allows to execute the algorithms in concrete domains. In Theorema, genericity is achieved in an elegant way by "functors", see [11, 12], that are similar to the functors in ML but slightly more general. The methodologic challenge consists in succeeding to have genericity and efficiency at the same time: In Theorema, algorithms and, in particular, generic algorithms are just particular predicate logic formulae whose execution is nothing else than the application of a small fraction of full predicate logic, namely the directed equational part ("rewriting"). In order to achieve efficiency, in the next version of Theorema, we will provide a compiler that compiles the Theorema predicate logic algorithms into Java. Recent experiments have shown that the speed-up achieved by compilation is drastic (a factor of several hundred).

An example of a functor is the functor NCP that takes a coefficient domain C and a domain of "terms" T and produces the domain $NCP(C,T)$ of noncommutative polynomials over C and T. In more detail, NCP defines algorithms for the operations $0, +, *, ...$ in $NCP(C,T)$ from the operations $0, +, *, ...$ in C and operations $1, *, ...$ in T. (In fact, each of the variants of

the notion of noncommutative polynomials, and each possible representation of polynomials, gives rise to a different functor). Also, various theorems on the properties of domains generated by certain functors in dependence on properties of the ingredient domains can be established. Hence, functors do not only "transport" bundles of operations to bundles of operations but also properties of operations to properties of operations. We call theorems that describe this type of property transportation "conservation theorems". In this view, a big part of the theory that is accumulated in cases like the one to be treated in this thesis can be viewed as a collection of conservation theorems. Special reasoning tools are available for this type of theorems in Theorema, more powerful ones should be added in the course of this thesis.

The *relationship of Gröbner bases theory and linear algebra* on words is a promising view for obtaining a drastic improvement of Gröbner bases algorithms. Practically, this opens the possibility for using efficient linear algebra algorithms (see for example the LinBox Project, [30]) in the reduction process w.r.t. multivariate polynomials. The positive computational effect has been demonstrated recently in an impressive way by the implementation of (commutative) Gröbner bases and its very successful application to cryptoanalysis in [22]. Theoretically, the relationship is not yet satisfactorily explored. We believe that results that are analogous to Habicht's univariate results, see [46], and subresultant theory, see for example [25]. should be possible for the multivariate (commutative and noncommutative) case. We proposed this idea already many years ago, for the first time in [8], but the details are rather difficult to pursue. A thesis, [26], along these ideas under the supervision of the proposer did not go sufficiently deep and revealed that a formal exploration, supported by automated reasoning tools, will be helpful for being able to keep track of the subtle proof details. Given the advances in formal computer-supported reasoning as provided by the Theorema environment, should result in a significant step forward in developing a generalized Sylvester matrix theory. This investigation is the major theoretical challenge of the proposed thesis.

The objectives of this thesis are demanding. Hence, probably, there will be not more time left for actively investigating one of the *topical applications of noncommutative Gröbner bases* in the frame of the thesis. However, interaction with the people working on the applications mentioned above should be pursued in the course of working on the thesis.

International Interaction

Work on the thesis should be carried out in interaction with the following research groups:

- *The group of J.C. Faugère, Univ. Paris VI*: Relationship between Gröbner bases and linear algebra, application in cryptography.
- *The LinBox Project, M. Giesbrecht, U. of Waterloo, Canada; E. Kaltofen, NCSU, USA; et al.*: fast linear algebra.
- *The SINGULAR Project, G.M. Greuel et al., U. of Kaiserslauter, Germany*: Advanced implementation of noncommutative Gröbner bases.
- *The group of M. Kreuzer, U. of Dortmund, Germany*: Gröbner bases and poly-cracker approach to cryptography.

- *Elsevier (Amsterdam), publisher of Journal of Symbolic Computation*: The result of this thesis, both as a formal mathematical theory (including its algorithmics) and as a benchmark and case study for the methodological philosophy of Theorema (and similar current systems and projects like, for example, [27] and [28]) will be an important input into a major project "Math Journals as Active Reasoning Agents", proposed by the thesis supervisor B. Buchberger, in cooperation with (Elsevier).
- *The Mizar Group, U. of Byalystok, Poland*: Formal mathematical theory exploration.
- *The Group of J.L. Ruiz-Reina, U. of Sevilla, Spain*: Formal verification of Gröbner bases algorithmics in ACL2.

Specific Educational Value of this Thesis for the PhD Candidate

In addition to the value of this thesis for computer algebra research and the application of computer algebra methods in various branches of mathematics (and, based on this, in science and technology), this thesis has a specific educational value for the PhD candidate because it trains, develops, and brings into coherence six different methodological capabilities in the mind of the student:

- *The Theoretical Aspect:* Develop a mathematical theory systematically and thoroughly and add nontrivial research (Gröbner bases and its relationship with linear algebra).
- *The Algorithmic Aspect:* Develop, verify, implement, and fine-tune algorithms.
- *The Methodologic and Software Technologic Aspect:* Use functors for generic programming.
- *The Formalization and Automated Reasoning Aspect:* Use and extend formalization and automated reasoning tools (of Theorema).
- *The International Aspect:* Interact with leading research groups worldwide.
- *The Application Aspect:* Apply the results to a topical application area.

Work plan

1st Semester:

- *Literature* study the literature as described in this proposal; extensively search the literature and compile a complete bibliography.
- *Theorema:* introduction to the formal mathematical theory exploration philosophy of Theorema and training in using the Theorema system.

2nd - 3th Semester:

- *Extend and Formalize the Theory:* formalize the various versions of Gröbner bases theory in noncommutative domains in the frame of the Theorema version of predicate logic; fill gaps in the theory; attempt formal verification of the theory by using (and extending) the formal reasoning tools of Theorema.

- *Design and Implement Domains and Functors:* design, implement, test, tune, and formally verify various versions of noncommutative polynomial domains and various versions of Gröbner bases algorithmics in these domains in a generic way using the Theorema functor approach.

4th - 5th Semester:

- *New Research:* Use the formal knowledge base for Gröbner bases theory and the reasoning tools built up in the previous step for a systematic research on the relationship between Gröbner bases and linear algebra along the generalized Sylvester matrix approach.
- *Integration:* Smoothly integrate the results into the formal knowledge base

6th Semester:

- *PhD Thesis Writing:* write and polish the PhD thesis; prepare presentations.

DK3 Bert Jüttler: Geometric Solvers for Polynomial Systems

Abstract

Robust algorithms for solving systems of polynomial equations, which are based on Bézier clipping and its variants [71, 76, 57, 68], find all roots in a bounded domain and have second order convergence for single roots. E.g., such techniques are needed for solving intersection problems in Computer Aided Design [63, 72], but they can also be useful for applications in robotics and numerical simulation, e.g., [60, 61].

Recently we formulated a new geometric algorithm for solving univariate polynomials via approximation by quadratic enclosures with good convergence rates: 3 for single and $\frac{3}{2}$ for double roots [52] . In particular, it performs very well in the case of two roots which are relatively close to each other. We plan to explore several extensions and related applications.

Current State of Research

A system of polynomial equations (polynomial system for short) of degree d in n variables $\mathbf{x} = (x_i)_{i=1}^n$ is a collection of n multivariate polynomials $\mathbf{p}(\mathbf{x}) = (p_1(\mathbf{x}), \ldots, p_n(\mathbf{x}))$ of degree d. In the generic case, its solution is a set of d^n points in $\mathbb{C}^n$ which satisfy $\mathbf{p}(\mathbf{x}) = 0$. Depending on the application, one is interested in the solutions for $\mathbf{x} \in \Omega$, where the domain Ω can be $\mathbb{C}^n, \mathbb{R}^n$, or some subset of $\mathbb{R}^n$. We are interested in numerical techniques for the case $\Omega \subseteq \mathbb{R}^n$, which are guaranteed to find all solutions. Clearly, several powerful techniques from the field of symbolic computation exist also. In this proposal we restrict ourselves to numerical techniques. All computations are to be done with floating point numbers.

The investigation of algorithms for solving polynomial systems has been an active research area for a long time. Many related references can be found in [67].

For instance, *homotopy techniques* form an important class of algorithms. These techniques (see, e.g., [64, 77]) start with the solutions of a simpler system with the same structure of the set of solutions. This system is then continuously transformed into the original system, and the solutions are found by tracing the solutions. Homotopy techniques are particularly well suited for $\Omega = \mathbb{C}^n$.

Another class of algorithm combines *bisection* steps with Descartes' rule of signs in order to isolate the roots [69, 74, 53].

The rich literature on roots of polynomials also contains various results on *enclosures* of polynomials and their roots, e.g., [56, 65, 75]. In particular, techniques of interval and affine arithmetic have been used to deal with uncertainties and numerical errors.

In this project we will focus on polynomial given in Bernstein-Bézier (BB) representation,

$$p(x) = \sum_{i=0}^{d} c_i \, \varphi_i(x), \qquad x \in [a, b], \tag{1}$$

with Bernstein polynomials $\varphi_i = \binom{d}{i} s^i t^{d-i}$, $s = \frac{x-a}{b-a}$, $t = \frac{b-x}{b-a}$ and real coefficients c_i. This representation forms an essential part of the technology for free-form curves and surfaces in Computer Aided Design [63, 54, 73, 69]. Compared to other representations, it has two main advantages.

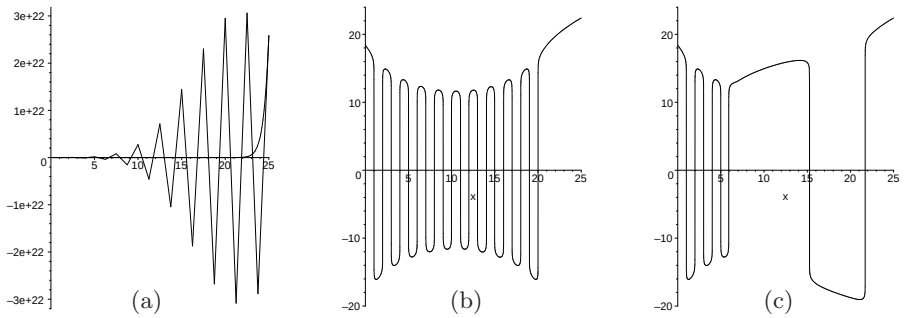


Figure 1: Numerical stability of the BB representation. The Wilkinson polynomial (a) and the effect of adding $10^{-8}\%$ coefficient error to the BB representation (b) and to the monomial representation (c). The latter two figures show the graphs of $\text{sign}(w)\log_{10}(1+|w|)$. While the BB representation preserves the root pattern (b), this is not the case for monomials (c).

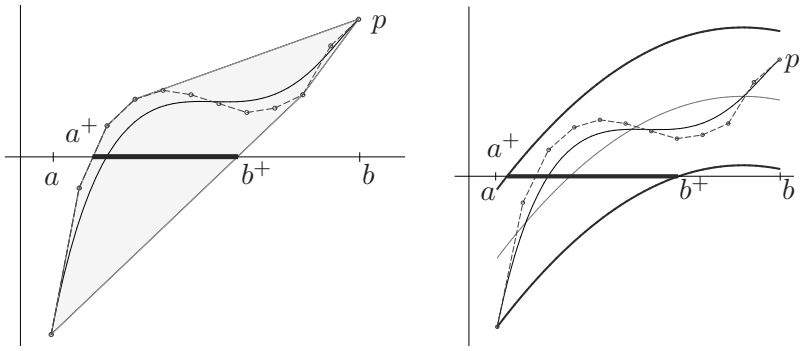


Figure 2: Bézier clipping vs. quadratic clipping. Left: Bézier clipping [71]. The convex hull property provides a smaller interval $[a^+, b^+]$ containing the roots. The algorithm proceeds by computing the BB representation with respect to the newly generated interval. Right: Quadratic clipping [52]. The same is achieved by using a quadratic enclosure.

First, the BB representation is *numerically stable*, see [55]. This observation also applies to evaluation and to the computation of BB representations with respect to subdomains via de Casteljau's algorithm or other suitable algorithms (cf. [66]). As an example, in Fig. 1 we consider the Wilkinson polynomial $w(x) = \prod_{i=1}^{20}(x-i)$ and compare the stability of the BB representation with respect to the interval $[0, 25]$ with the stability of the usual "monomial" representation (with respect to powers of x).

Second, the BB representation provides the *convex hull property*; the graph of the polynomial (1) does not leave the convex hull of the control points $\{(\gamma_i, c_i)\}_{i=1}^n$, $\gamma_i = (1-\frac{i}{d})a + \frac{i}{d}b$. Consequently, all roots of p in $[a, b]$ are located within the intersection of the convex hull with the x-axis, see Figure 2, left. This observation, combined with subdivision, has been used to formulate fast (achieving quadratic convergence for single roots) solvers for univariate polynomials [71].

Solutions to systems of polynomial equations are needed frequently in Geometric Com-

puting with free-form curves and surfaces. Various subdivision-based algorithms with linear convergence have been formulated [53] and perform remarkably well, due to efficient implementations. Multivariate versions of Bézier clipping exist [69, 76] and have found their way into industrial software, such as commercial CAD systems.

Recently, we formulated a new method for the univariate case [52]. This method is based on a simple and efficient generation of quadratic enclosures, see Fig. 2, right. In each iteration, the next interval containing the roots is found by solving a single quadratic equation. Recall that all computations are done in floating point numbers. Evaluating a square root is therefore assumed to take constant time. In the case of double roots, the convergence rate is still $\frac{3}{2}$, while the method achieves even cubic convergence for single roots.

Clearly, double roots are unlikely to be present in practice, when the input is specified by floating point coefficients. However, the superlinear convergence for double roots is also an advantage for the case of a situation near to a double root. In the case of two neighboring real roots, Bézier clipping slows down to linear convergence, until the roots are isolated by subdivision steps (and similar for two neighboring conjugate-complex ones). The novel method provides superlinear convergence throughout.

Objectives and Methods

The planned Ph.D. project will structured in four parts.

Part 1: Multivariate algorithms. The goal of this part is to generalize the univariate algorithm of [52] to polynomial *systems*. We assume that the domain Ω is a box. The case of general domains (including unbounded ones) can be reduced to this situation, by a parameter transformation. Two approaches are to be explored.

First, we will use n *linear* enclosures of the polynomials, where n is the number of equations. Some very preliminary tests are described in [51]. As indicated by them, this approach is expected to provide quadratic convergence for single roots. The existing techniques achieve this convergence rate only with the help of additional preprocessing steps, as used in [69]. Several possibilities for choosing the linear enclosures will be explored, including L^2 best approximation, as in [52], and other techniques [56].

Second, we will use combinations of $n-1$ linear enclosures and one *quadratic* enclosure. By using a single quadratic enclosure, the new box containing the roots can be found by solving a single quadratic equation, as in the univariate case. Still, the enclosures are to be chosen such that they maintain superlinear convergence for double roots.

For both approaches we will analyze the theoretical convergence rates for the cases of single and multiple roots, and the computational complexity with respect to the degree and to the number of equations. We will compare the methods with existing techniques (e.g., with other iterative techniques and with homotopy methods) with respect to various criteria: convergence rates, complexity with respect to the degrees, computing times (based on experimental implementations of the new methods) and number of operations. As a byproduct of these comparisons we will explore the feasible ranges of n (number of equations) and d (degree of the system) which can be dealt within reasonable computing time.

Part 2: Applications. This part is to demonstrate that the new algorithms are capable of solving real-world problems involving polynomial systems. We will apply the algorithm to various

concrete problems from Geometric Computing and other fields. The problems to be addressed include intersection problems in Computer Aided Design [63, 59], the topology analysis of planar algebraic curves [58], a special polynomial system arising in computational elastoplasticity [60] (jointly with the team of DK4), and the inverse kinematics of general 6R robotic manipulators. For the latter problem, recent results show that this can efficiently be formulated as a polynomial system of relatively moderate degree with two equations ($n = 2$) [61], while the elimination of one more variable (which gives a single polynomial of degree 16) is quite expensive. Computing all solutions may help to detect singular positions of the robot, where several roots coincide.

Part 3: Robust computing. The goal of this part is to adapt the algorithms from Part 1 to the case of polynomial systems, where the coefficients are only known with limited accuracy. Here we will systematically use techniques from interval and affine arithmetic (cf. [70]). In addition we will analyze the propagation of rounding errors.

On the one hand, we analyze how to obtain valid enclosures if the coefficients of the given polynomials are given with limited precision. On the other hand, we will modify the clipping step in order not to lose any roots, by applying an additional analysis (e.g., detection sign changes of the BB representation) to the boxes which are clipped away. The latter approach may help to reduce the use of interval arithmetics.

Part 4: Higher order enclosures. Here, the aim is to formulate algorithms with superlinear convergence for roots of higher multiplicity. This will adapt these algorithms to root clusters containing more than two roots.

In the univariate case we will look at cubic and quartic enclosures. The new intervals containing the roots are then found by solving equations of degree less than four, where closed-form solutions still exist. It is also planned to extend this approach to system of polynomials. Similar to the case of quadratic enclosures, special care is needed in order to make the computation of the next box computationally tractable.

Possible extensions. Various possibilities for additional research exist:

• Generalization to systems of general non-linear equations. The classical Bézier clipping can be seen as a robust version of a Newton method, as the convex hull of the control polygon converges towards the tangent of the curve. By replacing the tangent of the curve with an osculating geometric primitive (circle, parabola,...) of higher order, higher-order geometric Newton methods can be found and should be analyzed.

• Clipping in other spaces of functions. BB-type techniques exist for spaces containing, e.g., trigonometric polynomials [62], and it should be possible to generalize the results about polynomial systems.

• Advanced computer hardware provides new possibilities (such as graphics cards, parallelization) and might lead to new classes of algorithms (planned cooperation with G. Haase, Graz).

• Various other *applications* of polynomial systems exist and are promising subjects for further research. In particular, this includes problems from numerical optimization.

• For certain applications it should be of some interest to extend the methods to the case of complex roots, $\Omega \subseteq \mathbb{C}^n$.

Work plan

The four parts progress from applications of existing techniques (linear enclosures for systems, higher order enclosures for univariate polynomials) to the exploration of new concepts (quadratic and higher order enclosures for systems). Additional impulses will be provided by studying concepts from interval analysis and by discussing relevant applications. The first three parts will be dealt with simultaneously. Part 4 is to be addressed later on.

DK4 Ulrich Langer: Nonstandard Finite Element Solvers for Second-Order Elliptic Boundary Value Problems

Abstract

We propose to investigate non-standard finite element schemes for solving second-order elliptic boundary value problems. The construction of these finite element schemes are based on boundary element technologies and interface-concentrated finite element techniques. The first approach allows us to treat polyhedral and even more general meshes, whereas the second technique can easily handle subdomains with complicated interfaces and/or complicated behavior of solution along these interfaces. The combination of both discretization techniques and their coupling with data-sparse boundary element discretizations are feasible. The construction of fast and highly efficient parallel solvers for the corresponding systems of algebraic equations is the ultimative goal of this project.

Current State of Research

In order to construct new finite element (FE) approximations to linear boundary value problems (BVP) for 2nd order partial differential equations (PDEs), like the potential problem and the linear elasticity problem, on very general meshes, we will borrow ideas from the symmetric domain decomposition (DD) boundary element (BE) method. The symmetric formulation originally proposed by M. Costable for FE-BE coupling [84] was then used by G. C. Hsiao and W. L. Wendland [87] to construct BE DD schemes. The proposer has contributed to the fast solution of such schemes [91, 83, 93, 92]. These schemes can be interpreted as a BE approximation to the skeleton variational formulation

$$\sum_{i=1}^{p} \langle S_i u|_{\Gamma_i}, v|_{\Gamma_i} \rangle = \sum_{i=1}^{p} \langle N_i f_i, v|_{\Gamma_i} \rangle \tag{2}$$

of the BVP under consideration, where here S_i denotes the Steklov-Poincaré operator corresponding to the PDE, N_i is the Newton potential operator, and $\overline{\Omega} = \cup_{i=1}^{p} \overline{\Omega}_i$, $\Omega_i \cap \Omega_j = \varnothing$, $\forall i \neq j$, is a non-overlapping DD of $\Omega \subset R^d$ (see also the survey paper [94] and the references therein). We will use the BE-DD formulation in order to construct new finite element schemes on polyhedral and even more general meshes. There are other approaches to construct approximation on polyhedral meshes, see, e.g., [90, 82] and the references therein. However, the potential of the symmetric BE DD method seems to be very promising. It can be interpreted as a local Trefftz method, i.e. as a finite element method working with ansatz-functions which are solution of the PDE on the finite elements. The BE technology allows us to generate the element stiffness matrices and the element load vectors with linear complexity.

Another interesting non-standard FE technology is the so-called boundary concentrated finite element methods (BC-FEM) introduced and investigated by B. Khoromskij and J.M. Melenk in [88]. This technique allow us to solve potential problems with smooth coefficients in domains with complicated boundaries as accurately as the corresponding standard finite element methods (FEM) but with a significantly smaller number of unknowns. Indeed, the total number of unknowns in the BC-FEM is proportional to $O(h^{-(d-1)})$ whereas the total number of unknowns in the standard FEM behaves like $O(h^{-d})$, where h and d denote the average discretization

parameter of the boundary and the spatial dimension, respectively. Local discretization error estimates in different norms can be found in [86]. Moreover, at least for Dirichlet problems, the stiffness matrices of the BC-FEM are significantly better conditioned than the usual stiffness matrices. This property was already discovered by H. Yserentant [98]. Efficient solution methods for the BC-FEM have been designed in [89, 88, 85]. Interface concentrated finite element methods (IC-FEM) are a combination of nonoverlapping domain decomposition (DD) methods with the BC-FEM that is used in the subdomains Ω_i in which the initial domain Ω is decomposed. Now we can admit piecewise smooth coefficients in the PDE that we are going to solve. Primal and dual iterative substructuring solvers for interface concentrated finite element schemes have been developed in [78].

Objectives and Methods

We now consider the subdomains Ω_e (usually characterized by the average diameter $H >> h$ in DD) as finite elements of an average mesh size $H = h$. The element stiffness matrices

$$A_e = D_e + (\frac{1}{2}M_e + K_e^T)V_e^{-1}(\frac{1}{2}M_e + K_e) \tag{3}$$

are now generated by the boundary element matrices D_e (hypersingular matrix), K_e (double layer potential matrix), V_e (single layer potential matrix) and M_e (mass matrix). The matrices D_e, K_e and V_e are dense, but of small size ! Similarly, the element load vectors f_e are generated by the use of Newton's potentials. After assembling, we obtain the global system

$$Au = f, \tag{4}$$

with

$$A = \sum_{e=1}^{p} R_e^T A_e R_e \quad \text{and} \quad f = \sum_{e=1}^{p} R_e^T f_e, \tag{5}$$

where R_e is the usual restriction operator mapping an global nodal vector to the local element vector and $p = O(h^{-d})$ is now the number of unknowns. This method is a Boundary Element based Finite Element Method (BEbasedFEM) and can be considered as a local Trefftz methods as was already mentioned above. It is clear that this procedure admit very general meshes including polygonal and polyhedral meshes in 2d and 3d, respectively. A priori and a posteriori discretization error estimates as well as efficient methods (e.g. Algebraic MultiGrid (AMG) methods) for solving these exotic FE equations are certainly challenging problems for studying in the framework of a PhD thesis. The development of the corresponding software also requires additional ideas. This new approach can be developed in different directions: elements with special features, p-versions (no inner nodes !), Discontinous Galerkin (DG) and hybridization (non-matching grids), new applications (e.g. Stokes, Maxwell etc). Here we will continue the cooperation with the projects in symbolic computation (fundamental solution, integration, special functions, AMG), with the integration of direct and inverse solution techniques and the work on geometrical problems started in the SFB F013.
There are only a few papers on boundary and interface concentrated finite element methods which have already shown the potential of this approach. We propose to investigate modifications of the interface concentrated finite element method for problems with a complicated

structure of the solution along the interfaces and with moving or even a priori unknown interfaces. For instance, the latter case arises from treating elasto-plastic problems (see SFB project F1306), topology optimization problems (see SFB project F1309), or parameter identification problems.
Interface concentrated finite element schemes can be generated by the boundary element technology discussed above and can be coupled with data-sparse boundary element approximations.

Work plan

The following working program (36 months = 3 years) is designed for one PhD student, although the topics briefly described above provide research work for one or two more PhD students. We suppose that the PhD students are familiar with the basic knowledge on elliptic PDEs and their numerical solution via FEM as it is provided in our master courses and as it is presented in the books [79, 80, 81]. Usually one cannot suppose that the students are familiar with advanced boundary element and domain decomposition techniques.

1. Study of the literature on BEM, e.g. the books by S. Sauter and C. Schwab [95] and O. Steinbach [96], and on Domain Decomposition Methods [97] as well as of the corresponding journal papers relevant for the work on the PhD thesis **(months 01 - 12)**

2. Training research work on BEbasedFEM, IC-FEM and combinations BEMbased-IC-FEM coupled with BEM for the 2D potential equation as well as software development on basis of our 2D DD FEM-BEM software **(months 03 - 12)**

3. Construction and Analysis of BEbasedFEM for the potential equation in 3d, a priori and a posteriori error analysis, fast solvers **(months 06 - 24)**

4. Development of primal, dual and primal-dual DD solvers **(months 18 - 30)**

5. Development of DD software for the 3D potential problem and numerical testing **(months 24 - 36)**

6. Completion of the PhD thesis (**(months 31 - 36)**

This PhD student supported by the DK will closely cooperate with other PhD students of the DK (in particular, with the PhD students of DK6 and D12) and of the Institute for Computational Mathematics as well as with the group of Prof. Steinbach at the TU Graz. We can hopefully associate further PhD students to the DK supported by other institutions. One topic of research work can be devoted to the use of the boundary element technique in the IC-FEM (BEbased-IC-FEM) and the coupling with data-sparse BEM for 3D potential problems. Here we will cooperate with Dr. Eibner (TU Chemnitz), Dr. Khoromskij (MPI Leipzig), Prof. Melenk (TU Vienna) and Prof. Steinbach (TU Graz). Another PhD topic is the use IC-FEM in the case of unknown or/and moving interface in 2D and 3D that requires a detection mechanism of the unknown interface as well as a smart implementation. The extension of these non-standard finite element technologies to other problem classes like elasticity equations, Stokes equations, Maxwell's equation etc. is, of course, feasible and can be investigated in the second period of the DK.

DK6 Peter Paule: Computer Algebra Tools for Special Functions in Numerical Analysis

Abstract

We propose the development of computer algebra tools for special function manipulation. For many years the proposer's group has been working in this area; see the web page of the RISC Algorithmic Combinatorics group [99]. Despite these efforts and other recent developments briefly described below, this research area is still in its early stage and much remains to be done. Being a subproject of the DK, particular emphasis will be put on tools that help in solving problems arising in numerical analysis. For example, in connection with hp finite element methods one typically encounters problems related to (multiple) definite integrals and inequalities involving special functions.

Current State of Research

A survey of the state of art is given in the forthcoming DLMF computer algebra chapter [100], jointly written by the proposer and F. Chyzak. Besides being author, the proposer is also associate editor of the DLMF [101], the Digital Library of Mathematical Functions, currently edited at the U.S. National Institute of Standards and Technology (NIST) as a completely revised version of the widely spread 1964 *Handbook of Mathematical Functions* [102] edited by Abramowitz and Stegun.

The beginnings of modern development trace back to the PhD thesis of M. Fasenmyer (often called Sister Celine). E. Rainville devotes a whole chapter to the description of her ideas in [103], the first monograph devoted entirely to special functions. D. Zeilberger was the first who fully recognized the algorithmic content of Fasenmyer's method. His holonomic systems approach [104], his creative telescoping algorithm [105] based on Gosper's algorithm [106], and the article [107] with H. Wilf can be viewed as the breakthroughs which initialized the modern development of the field. Symbolic summation has received particular attention. See, for instance, the work of S. Abramov starting with [108], of M. Karr [109] and C. Schneider's extension of it starting with [110], of the proposer, e.g. [111], of M. Petkovšek starting with [112], and of many others.

Concerning more general aspects of special functions, including differentiation and integration, outstanding work has been done by B. Salvy and P. Zimmermann [113], N. Takayama, e.g. [114], and F. Chyzak who, beginning with [115], has started to execute the research program described by Zeilberger in [104]. But it seems that this more general territory has been much less explored than symbolic summation. There are several possible explanations of this view. One of them is due to the following observation.

Integrals and symbolic summation. Having efficient symbolic summation tools at hand, one might succeed in deriving a suitable representation for a given definite integral by transforming it into a summation problem. In practice, this technique has a good chance to work if the integral involves discrete (and sometimes also continuous) parameters.

An example where, following this strategy, a simpler representation, i.e., in terms of simpler functions, was found is [116]. There the definite integral under consideration arose in estimating the entropy of a physical process.

An example where, following this strategy, a (simple) recurrence with the given integral as solution was found is given in [117]. The problem arose in the context of finite element methods, more precisely, in the construction of edge-based high-order basis functions: Let $L_i(x) := \int_{-1}^{x} P_{i-1}(s)ds$, with P_i being the Legendre polynomials, and where $i \geq 2$ and $x \in (-1, 1)$. For $y > 0$ consider

$$\varphi_i^{(1)}(x, y) := \frac{1}{2y} \int_{x-y}^{x+y} L_i(s)ds.$$

Define

$$\varphi_i(x, y) := \varphi_i^{(2)}(x, y) - \frac{2y}{1 + x + y} \varphi_i^{(2)} \left(\frac{x + y - 1}{2}, \frac{1 + x + y}{2} \right)$$

where

$$\varphi_i^{(2)}(x, y) := \varphi_i^{(1)}(x, y) - \frac{2y}{1 - x + y} \varphi_i^{(1)} \left(\frac{1 + x - y}{2}, \frac{1 - x + y}{2} \right).$$

It turns out that the $\varphi_i(x, y)$ for $i \geq 6$ satisfy a linear recurrence of the form

$$\varphi_i = a_i x \varphi_{i-1} + (b_i + c_i(x^2 - y^2))\varphi_{i-2} + d_i x \varphi_{i-3} + e_i \varphi_{i-4}$$

where the coefficients $a_i, \ldots, e_i$ are rational functions in i over the integers.

Such recurrences can used for efficient evaluation of basis functions. The problem to find — and to prove (!) — such recurrences has led us to the development of new summation methods in the context of difference fields; see e.g. [118] and [119]. Namely, for the problem given above, one is able to invoke symbolic summation since the crucial $\varphi_i^{(1)}$ can be written as a difference

$$\varphi_i^{(1)}(x, y) = S(x + y) - S(x - y)$$

of hypergeometric sums S of the following form:

$$S(z) = -\sum_{k=0}^{i} \frac{2^{-2k+i-1} z^{-2k+i+1} (-\frac{1}{2})_i (-i)_{2k-1}}{y\, k!\, i!\, (\frac{3}{2} - i)_k}$$

where $(x)_n = x(x + 1) \cdots (x + n - 1)$ denotes the nth rising factorial.

In [117] similar further examples, in connection with low energy vertex functions, are given.

Needless to say that this strategy of transforming integration into a summation problem does not always work. Even in cases where such a transformation can be carried out, the resulting sum expressions may turn out to be intractable. Hence an extension of the algorithmic tool-box is desirable. Of special DK interest are those problem classes that arise in interaction with DK scientists in numerical analysis, in particular in the context of project DK4 by Ulrich Langer.

Inequalities. Another challenge is the algorithmic treatment of *inequalities* involving special functions. No general approach to this problem area was known until recently, when first steps in this direction have been made by members of my research group at RISC.

Based Collins' cylindrical algebraic decomposition (CAD) [120], S. Gerhold and M. Kauers in [121] developed a procedure for proving special function inequalities involving a discrete parameter. Their method has been implemented within Kauers' *SumCracker* package [122], written in Mathematica. A typical application is a computer proof [123] of the celebrated inequality of P. Turan [124] which reads as follows: For $n \geq 1$ and $x \in [-1, 1]$,

$$P_n(x)^2 - P_{n-1}(x)P_{n+1}(x) \geq 0$$

where the $P_n(x)$ are the nth Legendre polynomials. The same method also led to an optimal improvement concerning a lower bound for the Turan-Legendre expression; see [125].

In [126] V. Moll considered a certain representation of quartic integrals, namely,

$$\int_0^\infty \frac{1}{(t^4 + 2xt^2 + 1)^{m+1}} dt = \frac{\pi}{2^{m+3/2}(x+1)^{m+1/2}} p_m(x)$$

with polynomials $p_m(x) = \sum_{l=0}^m d_l(m)x^m$, $m \geq 0$, given by a (finite) binomial double sum as

$$p_m(x) = \sum_{j,k} \binom{2m+1}{2j} \binom{m-j}{k} \binom{2k+2j}{k+j} \frac{(x+1)^j (x-1)^k}{2^{3(k+j)}}.$$

After expansion of $(x+1)^j(x-1)^k$ in terms of powers of x, the coefficients $d_l(m)$ are given as a binomial triple sum. Moll was able to prove that $d_l(m) > 0$ for $0 \leq l \leq m$. In addition to positivity, he conjectured log-concavity for the $d_l(m)$, i.e., for $0 < l < m$,

$$d_{l-1}(m)d_{l+1}(m) \leq d_l(m)^2.$$

In [127] M. Kauers and the proposer were able to give a computer proof of the positivity of the $d_l(m)$ using K. Wegschaider's algorithm [128] and its implementation, the package *MultiSum* written in Mathematica. In addition, in the same paper a computer-assisted proof of Moll's log-concavity conjecture is given, obtained by a combination of the Gerhold-Kauers method with *MultiSum*.

Objectives and Methods

For the first DK period major research topics are: *(i) the design of algorithms for simplifying multiple-integrals; (ii) the design of provers for special function inequalities.*

Topic (i). A promising approach within the proposer's group is [129]; however, there are still problems (like efficiency) that need careful investigation. Also alternative approaches, based on (non-commutative) Gröbner basis techniques, e.g. by Chyzak [115], [130], by Chyzak and Salvy [131] and by Takayama [114] must be considered. A concrete interdisciplinary subtask will serve as a major stimulus for this work, namely, *the use of computer algebra in developing high order finite element methods.* I.e., the successful SFB collaboration [117], between the proposer's group and Langer's numerics group (DK4), should be continued. It already resulted in a significant speed-up of a recent FEM approach. Now, variations like the use of other orthogonal polynomials than the Gegenbauer family should be investigated. The possibility to achieve similar speed-ups of alternative high order approaches, e.g. [133], should be explored.

Another subtask concerns the careful investigation and analysis of techniques to transform integrals into sums, and vice versa. In this context, representations like Mellin-Barnes integrals for hypergeometric series, together with Mellin transformations, might play an important role; see [132] for background information on classical methods.

A further subtask is to develop an integration analog to Wegschaider's *MultiSum* refinement [128] of the Fasenmyer/WZ approach [107]. In this context variants of the Fasenmyer method as decribed in Rainville's [103] should be considered.

Topic (ii). Despite recent achievements like the computer-assisted proof [127] of Moll's long-standing log-concavity conjecture described above, this kind of research is still at its beginnings. Applicability and possible extensions of the Gerhold/Kauers [121] method needs to explored further. For instance, the following inequality due to J. Schöberl resisted any computer (and human!) attack so far: Let $P_n(x)$ again denote the nth Legendre polynomial. Then Schöberl conjectured that for $n \geq 0$ and $-1 \leq x \leq 1$:

$$\sum_{j=0}^{n}(4j+1)(2n-2j+1)P_{2j}(0)P_{2j}(x) \geq 0.$$

This problem arose in numerical analysis, more precisely, in a new convergence proof for a certain high order finite element scheme. For further background information and asymptotic observations see [134].

In view of Schöberl's problem, alternative methods for proving special function inequalities are welcome. Possible alternatives are based on the idea to use Fasenmyer/WZ approaches (and generalizations like [129]) to assist in solving *connection coefficient* ([132]) problems. For example, the first proof (by de Branges) of the Bieberbach conjecture used an inequality by R. Askey and G. Gasper as an important ingredient. Following its proof as described in section 7.4 of [132] one can see that the underlying structure is nothing but a connection coefficient problem.

Work plan

A major stimulus for the proposed research are concrete demands originating from work in numerical analysis, in particular in Langer's project DK4. As a consequence, we restrict ourselves to give only a rough sketch of possible major blocks of tasks. Obviously, in the first DK year, the initial phase is devoted to a thorough study of available computer algebra tools for special functions.

- A systematic investigation and analysis of techniques to transform integrals into sums, and vice versa, should be carried out. Representations of Mellin-Barnes type together with Mellin transforms should be also considered. A Mathematica prototype implementation of Chyzak's extension [130] of Zeilberger's algorithm should be produced. (Subtasks related to *topic (i).*)

- A (rudimentary) implementation (in Mathematica) of an integration analog to Wegschaider's *MultiSum* should completed. (Subtasks related to *topic (i).*) — Applications of *MultiSum* and its integration analog with respect to special function identities and inequalitites

(e.g., connection coefficient problems) should be explored. (Subtasks related to *topics (i) and (ii)*.)

- One can expect that a proper combination of multi-sum algorithms with Collins' CAD, as in the proof [127] of Moll's conjecture, should be more widely applicable. A systematic analysis of this aspect should be carried out. (Subtasks related to *topic (ii)*.)

It should be noted that each of the topics (i) (special function integration) and (ii) (special function inequalities) would be suitable as stand-alone PhD thesis topics. But there are sufficiently many interesting scientific connections between these two areas that justify to view them as one block. However, in case we are able to associate another PhD (financed from other sources than the DK) to project DK6, the topics could be kept more separate and would provide an ideal forum for these two students to cooporate.

DK8 Ronny Ramlau: Nonlinear regularization methods for the solution of linear ill-posed problems

Abstract

In the proposed project we aim at studying solution methods for linear ill-posed problems. We want to investigate non-linear methods since they seem to be better suited for the reconstruction of functions which are spatially inhomogeneous. In particular, we will focus on two-step methods where a data preprocessing step is followed by a reconstruction step. Thus, for the operator equation $Kf = g$ and possibly noisy data g^δ a solution is constructed as

$$f_{\alpha,\lambda} := T_{\alpha,\lambda} g \quad \text{with} \quad T_{\alpha,\lambda} = R_\alpha S_\lambda \ .$$

Herein $S_\lambda : Y \to Y$ denotes the data estimation defined on the data side and $R_\alpha : Y \to X$ denotes the reconstruction operator.

We are interested in the question which methods are suitable for both steps, how the combination can be achieved and what special results on parameter choice rules, convergence rates and computational costs can be proved.

Current State of Research

Inverse ill-posed problems with linear and non-linear operators have been studied extensively in the last decades, e.g. [135, 136]. For linear operators, most of the used regularization methods like Tikhonov regularization are linear. However, motivated by the fact that linear methods do not perform satisfactorily when $f(t)$ is spatially inhomogeneous, non-linear methods have been investigated in recent years. Some approaches towards non-linear methods based on wavelet theory are given in [137, 138, 139, 141, 142]. A wavelet-based approach, where the observed data are expanded directly in a wavelet series, is given in [139]. In this work a combination of wavelet shrinkage and Wavelet-Galerkin projection is considered. Based on this idea, we studied the regularization of linear ill-posed problems in two steps: a data estimation step (e.g. wavelet shrinkage) followed by a reconstruction step [141, 143, 144, 145]. A basic two-step method is given in [140] where the authors interpret classical linear regularization methods as a combination of the pseudoinverse and a smoothing operator in either order. In [140], both steps of the regularization method are based on the singular system of the operator and no information about smoothness properties of the exact data or about the noise model are used. In [141, 143] we considered a general (linear, compact) operator K and studied the combination of wavelet shrinkage and Tikhonov regularization. Wavelet shrinkage is chosen as a method particular well adapted to the smoothness properties of the unknown exact data and Tikhonov reconstruction is chosen as a method adapted to the properties of the operator (via its singular system). In this context we introduced the idea of *fractional filter functions* for classical regularization methods [143].

Wavelet shrinkage can be done by different thresholding operators. In [141, 143] we considered hard shrinkage and specified the noise to be additive white noise. Shrinkage estimates also exists for other noise models, for Poisson noise see [146, 147, 148]. Different ways of thresholding the wavelet coefficients have been studied in recent years: Besides the hard shrinkage and the

soft shrinkage also interpolation in between these two thresholding operators exists [149]. If additional information on the signal (signal pattern) is available one can also construct wavelets matching the given pattern [150]. Wavelet shrinkage is also used in [151] where the authors study regularization methods for linear inverse methods with a Besov norm sparsity constraint. The corresponding regularized solution is computed by an iterative algorithm (Landweber) with nonlinear shrinkage applied in each iteration step. In [152], we have also used sparsity constraints for the regularization of ill-posed problems. The special case that the inverse problem consists in deblurring and denoising an 2-dimensional image is studied e.g. in [153].

An important point in studying inverse problems is the *degree of ill-posedness*. An operator equation $K : X \to Y$ might be well-posed for $X = L_2$, $Y = H^t$ but ill-posed for $X = L_2$, $Y = H^\tau$ with $\tau < t$. To take into account that the degree of ill-posedness of an operator equation varies with the considered function spaces, inverse problems have been studied in a Hilbert scale framework. This was initiated in [154], since then inverse problems in Hilbert scales have been studied extensively [155, 156, 157, 158, 159, 160, 161].

A real world application for regularization methods is SPECT (Single Photon Emission Computerized Tomography), a problem from medical imaging. Indirect measurements of an activity function f are modeled by the attenuated Radon transform where the attenuation is due to the body tissue μ. For known μ, e.g. from a simultaneous CT scan, the problem of recovering f is linear and classical reconstruction methods can be applied. These efforts have been boosted by the development of a inversion formula for the attenuated Radon transform, first given by Novikov [162, 163, 164]. Based on the inversion formula, Kunyansky et. al. [165, 166] designed a reconstruction algorithm that can be seen as a generalized filtered backprojection. Unfortunately, the algorithm turned out not to be as stable as the filtered backprojection for the classical Radon transform. Recently some effort has been made to stabilize the method by using statistical noise properties of the SPECT measurements [167].

Objectives and Methods

The proposed project is concerned with two-step methods for linear ill-posed problems $Kf = g$ where a data smoothing operator S_λ is followed by a reconstruction operator R_α. For given noisy data g^δ an approximation to the exact solution is defined as $f^\delta_{\lambda,\alpha} = R_\alpha S_\lambda g^\delta$.

Within the first period of the DK we plan to investigate the following topics:

1. Generalization of two-step methods,
2. Fractional filter operators for the reconstruction step,
3. Development of a-posteriori parameter choice rules,
4. Introduction of a unifying theoretical background,
5. Characterization of smoothing operators,
6. Investigation of a combination of data preprocessing and cg-method,
7. Applications of two-step methods (e.g. to SPECT).

Topic 1: We want to generalize two-step methods regarding noise models, shrinkage operators and reconstruction operators. In many applications we encounter noise models different from the so far considered white noise, e.g. colored noise or Poisson noise, which is in particular important for applications in medical imaging (SPECT, Topic 7). The noise model influences the way of measuring the overall reconstruction error. E.g., If an L_2-estimate for the data estimate is available the reconstruction error is measured in the norm whereas for white noise the expectation of the norm is computed.

In order to adapt two-step methods to other noise models, we want to enlarge the class of possible smoothing operators (Topic 5). For that, we will explore the approximation properties of appropriate (wavelet or other) bases in the presence of the considered noise. As one starting point we want to study the interpolation between wavelet soft and hard shrinkage. Another important point is the construction of so-called *optimally matched wavelets* which are designed to match given patterns (e.g. additional information on the signal). For these special wavelets the corresponding scaling coefficients have to be computed depending on the pattern. We want to use methods from symbolic computation for a fast and efficient realization of this task.

Since we do not aim at denoising on its own but as the first step in a two-step method for the solution of ill-posed problems we have to make sure that the link between the smoothing and the reconstruction operator is working. This is part of Topics 4, 5.

Topic 2: As one realization of the reconstruction operator in two-step methods we aim at fractional filter methods since they allow a reconstruction close to the problem. In particular the typical oversmoothing of standard methods can be prevented, such that e.g. discontinuities can be reconstructed more accurately. For the practical usage of the method, we want to develop algorithms that allow an efficient evaluation of fractional powers of an operator. One approach to this problem involves the product of series expansions. For this we want to exploit methods from symbolic computation, e.g. transformations to accelerate convergence, to achieve fast and stable formulas for the evaluation of the series product.

Furthermore, we are interested in the variational formulation of the fractional filter approach. So far we use fractional powers of matrices for the evaluation; a variational formulation will give theoretical insights in the relevant function spaces (Topic 4) and will enable us to apply standard minimization algorithm for the computation of a solution. The variational formulation is also useful to adapt fractional methods to nonlinear problems. However, nonlinear operator equations are planned for the next stage of the DK.

Another generalization of the fractional approach is to adapt the fraction parameter γ to local properties of the signal. The standard Tikhonov method ($\gamma = 1$) performs well for smooth signals but generally oversmoothes sharp or fine features of the signal (e.g. discontinuities). Since the fractional Tikhonov method needs more computational time, we would like to use it only for non-smooth parts of the signal. To realize this we want to use frames in the data preprocessing step to gain a representation of the signal separating smooth and non-smooth parts. The reconstruction should then be done with different fraction parameters for the smooth part ($\gamma = 1$, standard method) and the non-smooth part ($\gamma < 1$, fractional method). The resulting method is nonlinear and more flexible in adapting to local properties of signals.

Topic 3: A two-step method has (at least) two regularization parameters, one each for the data smoothing step and the reconstruction step. So far only a-priori rules exists for the

combination of wavelet hard shrinkage and (fractional) regularization methods. These a-priori rules depend among others on the smoothness of the exact solution and on the noise level; information which is not given when dealing with real world problems (Topic 7). We want to investigate new rules that are adapted to the data structure as well as to the reconstruction and guarantee optimal convergence rates without explicit knowledge of the smoothness of the exact solution. In particular, we would like to investigate a-posteriori rules based on the discrepancy principle and the Lepskii principle which do not depend on the (unknown) smoothness of the exact solution. Furthermore, we are interested in the mutual dependence of the parameters of the two steps: if the data smoothing step results in a data estimate which is in the range of the operator then the generalized inverse of the operator could be applied directly and no regularization is necessary anymore in the reconstruction step. Such a dependence could also help answering the question of how to weight the two steps: is there, depending on the problem (function spaces, noise model) and the method (which data smoothing and which reconstruction), an *optimal* choice of the regularization parameters; e.g. a choice that minimizes the error constants? (Topic 4)

Topic 4: Two-step methods are defined as the combination of a smoothing operator and a reconstruction operator. This requires a link between the two operators, which is so far only studied exemplarily: The adaptation of wavelet shrinkage to standard regularization methods (Tikhonov, Landweber) requires a translation of the mutual additional information of the exact solution. For wavelet shrinkage, smoothness conditions in Sobolev or Besov spaces are used. For standard regularization methods, smoothness conditions are given as *source conditions* in spaces defined by the operator K. So far, the example of wavelet shrinkage and regularization methods was linked using the theory of Hilbert scales since the operator-defined spaces as well as the Sobolev spaces define a Hilbert space.

As the results are promising so far, we want to build up a theoretical framework for the more general and precise definition of each part of a two-step method and the link in between. For this, we want to start with Hilbert scales and then carry on to other spaces (Besov, Banach). Especially the combination of wavelet shrinkage and standard regularization method requires at the moment that the operator K smoothes with a certain stepsize both in Sobolev and in Besov spaces,

$$\begin{aligned} K : H^s &\to H^{s+t} \\ B^s_{pp} &\to B^{s+t}_{pp} \ . \end{aligned}$$

We would like to formulate this result in a non-Hilbert setting using Besov spaces only.

Since this topic is concerned with the underlying theory of two-step methods it is related to all the other topics (closest related to the other 'theory Topics' 1 and 5).

Topic 5: An inverse problem $Kf = g$ with noisy data $g^\delta \in Y \supset \operatorname{rg} K$ has a certain degree of ill-posedness, depending among others on the space Y which contains the noisy data. E.g., for white noise it is $Y = H^{-d/2}$ where d is the dimension of the problem.

In solving the inverse problem, we search for a stable reconstruction of

$$K : X \to Y \ .$$

Applying a smoothing operator S_λ yields a data estimate $\tilde{g}$ in a space $\tilde{Y}$ which is possibly closer to the range of K than the original data Y,

$$S_\lambda : Y \to \tilde{Y} \ .$$

This is related to Topic 4 since we want to define a smoothing operator as an operator acting along a scale of spaces interpolating in between the data space Y and the range of K. For an operator smoothing in Sobolev spaces, $K : H^s \to H^{s+t}$, and the white noise model, $g^\delta \in H^{-d/2}$, this can be achieved with a smoothing operator $S_\lambda : H^{-d/2} \to H^\eta$ with $\eta \leq t$.

Another point we want to study when using a data pre-smoothing is the influence on the degree of ill-posedness. Whether we solve $Kf = g$ from $g^\delta \in Y$ or from $\tilde{g} = S_\lambda g^\delta \in \tilde{Y}$ renders the degree of ill-posedness of the problem. If $\tilde{Y} = \operatorname{rg} K$ then the problem is not ill-posed anymore and the generalized inverse $K^\dagger$ can be applied directly to the data estimate.

Topic 6: One of the few existing nonlinear methods for the regularization of linear problems is the conjugate gradient method. A typical observation when using the cg method is that after only a few cg-steps one gets a good approximation which then gets really bad after only a very few more cg-steps. The number of possible cg-steps depends on the degree of ill-posedness of the problem. By using a nonlinear data presmoothing step, we aim at an improvement of the degree of ill-posedness of the problem (Topic 5) and expect also more stable performance of the cg method.

Topic 7: An ill-posed problem from medical imaging is SPECT. Hereby it is assumed that in one part of the body (e.g. the heart) a radiopharmaceutical emits photons, which is described by the activity function. This photons travel through the body, are attenuated by the surrounding tissues, which is described by the attenuation function μ, and are counted outside the body by a SPECT camera. The mathematical model for the measurements is the attenuated Radon transform,

$$g(\omega, s) = A(f, \mu)(\omega, s) = \int_{\mathbb{R}} f(s\omega^\perp + t\omega) e^{-\int_t^\infty \mu(s\omega^\perp + \tau\omega) d\tau} dt \ .$$

For known function μ the reconstruction of f from the measured data $g = A_\mu(f)$ is a linear problem for which an analytical inversion formula exists. This inversion formula is unstable when the measured data are noisy and a first attempt to stabilize the problem is to apply a two-step method with different kinds of data pre-smoothing and the inversion formula for the reconstruction. However, it might still be necessary to regularize the inversion formula. For that we have in mind to use fractional filter methods since they allow a reconstruction close to the problem. So, by adjusting the fraction parameter to the inversion formula for the SPECT operator we hope to get a stable reconstruction without loosing sharp or fine features.

Work plan

We summarize the work plan for the proposed DK 'Nonlinear regularization methods for the solution of linear ill-posed problems' as follows:

T1
- Data smoothing for different noise models;
- Approximation properties of appropriate data smoothing methods (interpolation soft & hard);

- Construction of optimally matched wavelets.

T2
- Acceleration of the computation of fractional powers;
- Variational formulation;
- Minimization algorithms of the functionals;
- Combination of frames and fractional filters.

T3
- Investigation of a-posteriori parameter rules (Morozov, Lepskii);
- Optimal link of the two regularization parameters;
- Weighting of the two steps.

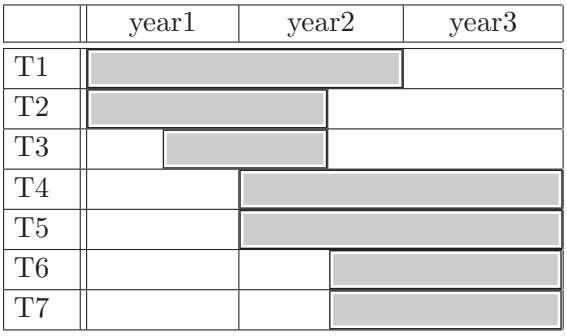
T4
- Investigation of the link between function spaces and source conditions;
- Besov space scales.

T5
- Influence of smoothing operators on the degree of ill-posedness;
- Measuring the degree of ill-posedness in the function space scales;
- Influence of the noise structure on the degree of ill-posedness.

T6
- Investigation of the dependence of the stability of the cg-method on the underlying function spaces;
- Convergence and convergence analysis for the combination of cg and data smoothing;
- Development of stopping rules depending on the smoothing step.

T7
- Numerical evaluation of the investigated methods;
- Application to real world problems;
- Reconstructions for SPECT with Poisson noise.

The starting time and the approximate processing time for each part of the project are scheduled as follows.



DK9 Josef Schicho: Symbolic-Numeric Techniques for Genus Computation and Parametrization

Abstract

A plane algebraic curve, given by a polynomial equation in 2 variables, is parametrizable by rational functions if and only if its genus is zero. For polynomials with real or complex coefficients, both the genus computation problem and the parametrization problem are severely ill-posed: a slight change in the coefficients may change the genus (which is always an integer) and may turn a parametrizable curve into a non-parametrizable one.

The goal of the proposed PhD project is to give symbolic-numerical algorithms that compute the genus, and if applicable to compute an approximate rational parametrization, in the sense of approximate algebraic computation (see [188]): The computed genus is the lowest genus of a curve with nearby coefficients, and if the computed genus is zero, then the computed parametrization is the exact parametrization of a nearby rational curve.

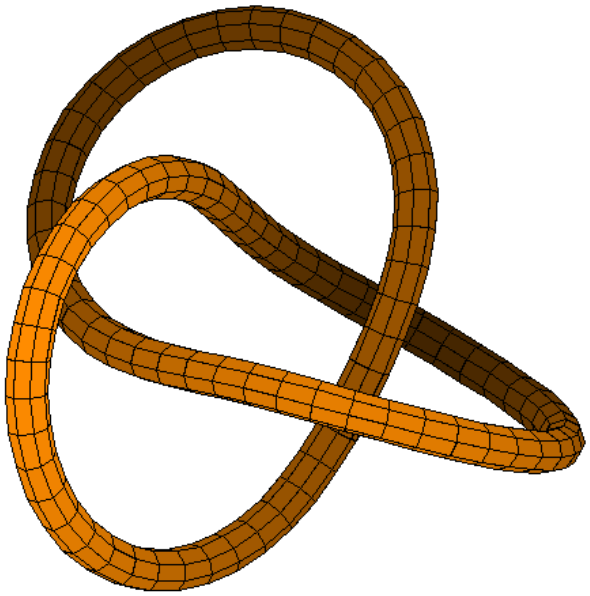


Figure 3: Link of the singularity $y^2 - x^3 = 0$.

In exact symbolic algorithms, the genus is computed via an analysis of the singularities, either by Puiseux expansion or by a resolution (see [186]). In the complex case, the singularities can be characterized by their link, which is defined as the intersection of the curve with a 3-sphere with sufficiently small radius (see Figure 1.1.4). When this radius is chosen carefully, one can compute the topological type of the link in a numerically stable way – this was indicated by a diploma thesis in the frame of the SFB "Numerical and Symbolic Scientific Computing" [180]. The main idea is to combine these informations on the singularities and the knowledge on the shape of the defining equation (degree, Newton polygon) in order to give an estimation of the genus in the above sense, which also decides the existence of an approximate parametrization.

Current State of Research

Symbolic algorithms for genus computation and curve parametrization are a classical topic in computer algebra, see for instance [182, 168, 187, 191, 179, 178]. There exist excellent implementations, for instance by M. van Hoeij in Maple or by F. Hess in Magma.

These algorithms/implementations use arithmetic of exact rational numbers or exactly represented algebraic numbers, and are therefore subject to the computational problem of expression swells. For many input polynomials of moderate size, the result cannot be computed because the computing time or the required memory space is too high; and for other examples of similar size, the coefficients of the computed parametrization are huge (in exact representation).

The development of approximate algebraic computation has been pushed by two facts. First, in many applications in science and engineering the input is only known up to a certain level of accuracy (for instance if the data come from measurements), and also the output is needed only up a certain precision (for instance the size of a pixel). This fact holds, in particular, for applications of curve parametrization in computer aided geometric design and geometric modeling. Second, numeric algorithms use floating point arithmetic, which is much cheaper than arithmetic for exact numbers, because expression swells are not possible at the level of coefficients. These two facts pushed research and lead to the symbolic-numeric algorithms for various classical problems in computer algebra, such as GCD computation [192, 174], factorization [172, 177], polynomial decomposition [173], and symbolic linear algebra (see the LinBox homepage `http://www.linalg.org/`). The last topic is especially relevant for curve parametrization, because solving a linear system is an essential substep in the existing symbolic algorithms.

Approximate rational parametrization has been considered in [184, 190, 176]. We define an approximate parametrization of a curve $F(x, y) = 0$ as an exact parametrization of a nearby curve. (The distance between curve may be measured algebraically, as the distance in coefficient space, or geometrically as Hausdorff-distance.) This agrees with general principles in approximate algebraic computation: the computed result should have a small backward error with respect to perturbations that preserve the structure (see [188]). In our case, a structure-preserving perturbation is one that preserves parametrizability, but one may also wish to preserve additional properties, like the multiplicity information of the singularities.

The algorithm in [184] gives an approximate parametrization by lines. Such a parametrization is possible iff the curve has a singularity of multiplicity $d-1$, where d is the degree of the curve. We call such curves "monoid curves". Numerically, a point p is an approximate m-fold point iff all partial derivatives up to order $m-1$ are small compared to $\|F\|$. If an approximate $d-1$-fold point exists, then there is a monoid curve in the vicinity, and [184] give explicit bounds for the Hausdorff-distance to the nearest monoid curve.

The algorithm in [176] works for cubics (cubic curves are rational iff they are monic). The authors consider a triangular region of interest and study the Hausdorff distance in that region. The nearest monoid is constructed by methods of approximation theory, using a Remes-type algorithm. In each iteration, one has to solve an interpolation problem. S. Fiedler-Le Touzé showed that there are sometimes geometrical obstructions for the existence of a solution of the interpolation problem with the correct topology [189]. If this happens, or if the nearest monoid is unacceptably far away from the input curve, then the suggestion in [176] is to decompose the region of interest and to split the input curve into pieces.

The characterization of plane curve singularities by their link is classical; an ex Milnor [183] investigated more generally the intersections of hypersurfaces in $\mathbb{C}^n$ with small spheres centered at an isolated singularity. His fibration theorem stated that the complement of the link in the sphere is a locally trivial C^∞ fibration, which implies a a strong topological condition on the link itself. In the curve case, one can remove the north pole from the sphere and apply stereographic projection and get a 1-dimensional compact manifold embedded in $\mathbb{R}^3$, i.e. a link in the sense of knot theory. The classification of knots and links is not yet solved, but for algebraic links – those that arise from singularities of plane curves – the theory is well understood. Two algebraic links are knot equivalent iff their Alexander polynomials coincide (see [175]). From the Alexander polynomial, one can compute the δ-invariant of the singularity by formulas in [171]. The δ-invariant of all singularities is exactly what is needed for the computation of the genus (see [170]).

For the numerical computation of the link respectively the δ-invariant, it is important to choose the radius of the sphere not too small, because otherwise the result may become wrong because of numerical errors. On the other hand, one should also not make it too big because the theory of the Milnor fibration holds only for sufficiently small radii. In the recent Diploma thesis by S. Kusper [180], this computation was done for some examples, and in the experiments there is always a large interval for which the δ-invariant is computed correctly. The thesis also contains suggestions to choose such radii automatically, but no analysis of the backward error.

Objectives and Methods

The goal of the proposed PhD project is to give symbolic-numerical algorithms for genus computation, and if applicable to compute an approximate rational parametrization, of the curve represented by a given polynomial $F(x, y)$ with real or complex coefficients. The coefficients are known with limited accuracy, and also the result must be interpreted as an approximate answer (in a sense which is specified below).

If the input polynomial is small, and the level of accuracy is high, then it is possible to compute with the approximate coefficients "along some symbolic algorithm": one takes such an algorithm and replaces each zero test by a test whether the absolute value is smaller than some tolerance ϵ. Then the computed result is approximately correct with high probability. Even certified results are possible using interval arithmetic, more precisely one can compute guaranteed lower bounds for the genus which become exact when the interval lengths approach zero.

If the level of accuracy is lower, then the simple approach described above does not produce good results. In this situation, the student should compute the "approximate genus", which is defined as the lowest possible genus of curve defined by a nearby polynomial (compared to the level of accuracy). If the approximate genus is zero, then he/she should compute a rational parametrization of a nearby curve of genus zero.

The set of exponents in the terms of the input polynomial, in particular the Newton polygon which is defined as the convex hull of the exponent vectors, is known exactly because this part of the input is discrete and not subject to numerical errors. Hence this information should be used. Exact symbolic algorithms that take advantage of the Newton polygon have been given in [170, 169]. The best upper bound for the genus of a curve with Newton polygon Γ is the number of interior lattice points of Γ (see [170]). If this upper bound is already zero, then the

Newton polygon is lattice-equivalent to the support of a polynomial which is linear in one of the variables, or to the support of a conic (see [185]). In the first case, there is an obvious rational parametrization because the equation can be solved in the variable that occurs linearly. For the second case, stereographic projection works, and a numerical algorithm is contained in [190].

For the computation of the real singular points of a real polynomial, efficient algorithms and implementations are available. Using the symbolic-numeric software Axel that has been developed by the Galaad team at INRIA Sophia-Antipolis, one can compute small boxes containing the singular points for polynomials of degree up to 100 with several thousand terms (see [181]). Additionally, singular points with complex coordinates have to be taken into account (even in the real case), hence these algorithms have to be adapted/extended to the complex case.

The next step is to compute an upper bound for the δ-invariant of a singularity, or – to be precise – an upper bound for the some of δ-invariants of singularities contained in a fixed small box (which has been computed in the previous step). Here, the stepping stone is the link of the singularity. To simplify the computation, we replace the sphere by the boundary of a polydisk

$$D_{\epsilon_1,\epsilon_2} := \{(x, y) \mid |x| < \epsilon_1, |y| < \epsilon_2\}$$

or by the boundary of a hypercube. As shown in [180], the link can be computed as a union of pieces each of which is a transversal intersection of two real surfaces in real 3-space. The choice of the radii ϵ_1 and ϵ_2 is a delicate matter. For the sake of numerical stability, it should be as big as possible, so that the intersection angle of the two surfaces is sufficiently big. On the other hand, the theorem of the Milnor fibration is only true for small radii (in particular, the polydisk or hypercube should not contain a second singularity). We think that a close inspection of the proof of this theorem and to related proofs will give the PhD student ideas to figure out the optimal choice.

The upper bounds for the δ-invariants give local contributions to a lower bound of the genus of the curve. It is not clear whether these local contributions are sufficient. This is equivalent to the statement that there is a nearby curve which simultaneously assumes all lower bounds for the δ-invariants. The construction of such a solution can be reduced to solving numerically a system of algebraic equations in the coefficients and in the coordinates of the singular points; the problem is made easier by the fact that an approximation to a (potential) solution is known (namely the input curve and the boxes containing the singularities). One reasonable approach is to try a few Newton steps, and to shrink the radii if there is a problem with convergency.

A different situation on which the student should focus is presented by polynomials of moderate size, say degree between 20 and 100, but with coefficients given exactly or at least with a sufficiently high level of accuracy. Here the main challenge is not to construct a nearby polynomial with lowest possible to genus, but to do devise a numerical method which scales well. For instance, elimination of variables is prohibited because this is too expensive on that scale. Allowed are computations like conversion to Bezier representation, subdivision (de Casteljeau's algorithm), Bernstein transformation, partial evaluation, linear substitution, univariate system solving. The algorithms in [181] give ideas how it should be possible to solve the problem under these conditions.

DK10 Wolfgang Schreiner: Formally Specified Computer Algebra Software

Abstract

We propose research on a semantic framework and supporting tools for the formal specification of computer algebra software written in statically untyped programming languages for the manipulation of expressions as they are used in the major computer algebra systems today. The focus of the work is to apply formal methods, rather than for verifying the correctness of the software, for finding and avoiding internal inconsistencies, in particular violations of method preconditions, which are typical indications of errors in the software (or at least of a lack of understanding of the developer).

Current State of Research

Computer algebra software has been repeatedly criticized concerning the correctness of the computed results [274, 228, 237, 241, 280]. While it is typically not the case that a result is "totally wrong", it is sometimes also not "really correct": it may only represent part of the answer or may be only valid under additional logical assumptions or in particular mathematical domains or under special interpretations of the arguments; however these caveats frequently remain unspecified. The main reasons seem limitations in the language between user and system incapable of expressing sufficient information such as domain information and logical dependencies [241], the unclear meaning of even fundamental notions such as "equality" [230] and most important a gross under-specification of the operations in the system documentation [280]. Consequently it is also for mathematical programmers difficult to build reliable software on top of computer algebra libraries or to employ computer algebra software as self-contained components [245] in contexts where no human is in the loop to continuously interpret the results and check their adequacy. This also the experience of the proposer and his coworkers who have in two recent FWF projects [262] worked on the development of an environment for formally describing, brokering, and executing mathematical services [204, 203, 202, 220], see also the supervised Ph.D. thesis [201].

The situation may be due to a separation between those users that are "just" interested in computing and those that are also inclined to deal with logical issues [241]. Nevertheless, there has also been considerable interest in combining the computational capabilities of computer algebra systems with the logical capabilities of theorem proving systems [218, 261, 211, 198, 221]. One branch of work provides *computer algebra systems with advanced reasoning capabilities* by connecting them to theorem proving systems: [196, 239] describes a Maple-PVS interface where Maple calls PVS to e.g. check the validity of a method call's precondition and postcondition; similarly [194, 195] presents a symbolic definite integral table where a given argument is matched against the entries in the table by invoking PVS to verify the necessary side conditions on the argument. Another branch of work provides *theorem provers with computing capabilities* by connecting them to computer algebra systems: in [243, 242] the proving assistant HOL uses Maple as an "oracle" to find answers to certain computational tasks which are then formally verified by HOL (checking an answer is often much easier than finding it); similarly [199] describes a connection of Isabelle and Maple and [200] a connection of Isabelle and the computer algebra

library Sum-It implemented in Aldor; here the answers are simply trusted to be correct. [273] presents a generic interface between the Omega proof planing system and computer algebra systems where the computer algebra system may return information that can be used to verify the computation. One may also attempt a much closer *integration of computing and reasoning*: e.g. the the reasoning system Theorema [276, 216, 215] built on top of Mathematica implements by its PCS method a proof heuristics that iterates phases of proving, computing, and solving on the basis of the algebraic methods provided by Mathematica; other examples of reasoning systems embedded into computer algebra systems are REDLOG [231] and Analytica [208, 226].

However, most of this work does in itself not contribute to increasing the trust in the correctness of the results returned by computer algebra software. At one extreme, one might simply accept this fact and ask for a separate check of every result and ultimately require that computer algebra software returns, together with its result, a *correctness certificate* that enables this check, e.g. an LF-style formal correctness proof like it is (optionally) returned by some arithmetic decision procedures [251, 263]; however, checking every result is costly and checking itself does not improve the correctness of the software. At the opposite side of the spectrum, one might also demand a radical change in the process of developing computer algebra software such that it becomes *correct by construction*: one may e.g. develop the software in a type-theoretic framework such that the specification of a method is denoted by its type and the fact that the method type-checks correctly guarantees its correctness with respect to the specification. A step in this direction is made in the Atypical project [279, 265, 266] where the type system of Aldor is modified such that its dependent types can be used to describe propositions and Aldor category specifications become axiomatic datatype specifications [278]; likewise [264] presents a type-theoretic elaboration of polynomial rings and the Gröbner bases algorithm. An alternative approach is to build a computer algebra system on top of a theorem proving system such that computations become rewriting proofs, see e.g. [223] for a computer algebra system built on top of HOL Light. One may also resort to program synthesis [207], where from a specification a program is constructed that is provably correct with respect to this specification, either manually by a sequence of stepwise refinement steps [249] or by some heuristically guided automatic process [214].

A more pragmatic approach is to equip a computer algebra system respectively language with a *formal specification language* and a corresponding logical framework: in [234, 235, 250] an integration of the behavioral interface specification language Larch with Aldor is presented; from Larch/Aldor programs, verification conditions are generated that are forwarded to the Larch prover for verification. The specification language of the Coq proving assistant has been variously used to define computer algebra algorithms and prove their correctness [277, 240, 259, 258, 260]; from the Coq definitions executable Ocaml programs can be automatically extracted. The FoCal (former Foc) project [267, 238, 213] has developed an axiomatic datatype specification language in which hierarchies of mathematical domains can be defined; a compiler extracts the computational parts as Ocaml programs and also generates verification conditions that can be interactively handled with the help a proving assistant; proofs are produced in the form of Coq scripts/terms that can be subsequently checked by Coq.

Much more than in computer algebra, in computer science interest in formal methods for modeling and reasoning has surged since the 1990s. Various specification languages have been developed, some of them programming-language independent e.g. VDM [248], Z [281], B [193],

Larch [256], Alloy [247], or also the Object Constraint Modeling Language OCL which is part of the UML standard [252]. Other formalisms are bound to particular programming languages such as Larch/C++ for C++ [256], Spark for Ada [205, 246], JML for Java [255], and Spec# for C# [205]. These languages are accompanied by corresponding tool sets that make use of automated reasoning techniques [217, 222] which has become possible due to the advances in SMT (satisfiability modulo theories) solving achieved since the late 1990s [272, 206]. The focus here is clearly not on verification of program correctness but on light-weight formal methods [269] e.g. to find by extended static checking [236, 224] possible runtime errors and internal inconsistencies in a program such as violations of specified method preconditions. Nevertheless, some environments provide integrated proving assistants that also support the interactive verification of complex correctness properties [210, 246].

Objectives and Methods

Admittedly the research described above has had up to now little impact on the actual practice of writing computer algebra software. Apart from those approaches that ask for fundamental changes in the computing principles or the development process, even the more pragmatic ones are bound to languages such as Aldor or Focal that are more advanced but also less used compared to the languages of systems like Maple, Mathematica, GAP, CoCoa, and others in which the vast majority of computer algebra software is written. Unlike languages with mathematically founded notions like categories (Aldor [197]) respectively species (Focal [267]) or magmas (Magma [212]) suitable for building abstract hierarchies of mathematical datatypes (see [257, 275, 219, 270, 225, 229] for related work) these languages are not even statically typed; they focus (in the tradition of Common Lisp) on the construction and manipulation of expressions compound of symbols and of values from specially supported datatypes such as unbounded integers. If formal methods shall influence the practice of writing computer algebra software, they have to be also applied to software written in these languages, and also provide some immediate advantage rather than only pointing towards a goal that is still far-away. The situation is analogous to that in computer science where remarkable success has been achieved since the focus has shifted from proving the full correctness of simple programs in rarely used languages towards the application of reasoning technologies to finding errors in complex programs in wide-spread languages.

The overall goal of the proposed research is therefore to work on a a specification language, a corresponding reasoning framework, and supporting tools for computer algebra languages that semantically operate on the level of expressions and for which any high-level interpretation as a mathematical datatype has to be especially constructed by a corresponding specification. This interpretation can be then used by the reasoning framework for checking the internal consistency of a program composed of multiple methods (and ultimately also form the basis for the verification of the program).

The core idea on which this work is based was already introduced by Hoare [244] and has been more precisely elaborated and further refined in [209, 253, 233, 232, 254]: in essence, for a concrete program type $\mathcal{C}$, a (partial) mapping $a : \mathcal{C} \to \mathcal{A}$ into an abstract mathematical type $\mathcal{A}$ is defined; a concrete program function $f : \mathcal{C} \to \mathcal{C}$ can be then specified by a precondition $P \subseteq \mathcal{A}$ and postcondition $Q \subseteq \mathcal{A} \times \mathcal{A}$ such that for every concrete argument $x \in \mathcal{C}$ with $P(a(x))$ the application $f(x)$ returns a concrete result $y \in \mathcal{C}$ such that $Q(a(x), a(y))$. The specification

(P, Q) of f thus operates, rather than on the concrete type $\mathcal{C}$, on the abstract type $\mathcal{A}$; the program function f has been thus specified as a mathematical function. The idea can be easily generalized to a heterogeneous scenario with multiple program types respectively abstract types, also the same program type may represent different abstract types in different contexts.

However, to turn the idea into a practical specification language, multiple questions have to be resolved. The first one, how to specify the semantics of the abstract type $\mathcal{A}$, is actually not crucial: any algebraic specification language in the tradition of OBJ3, Larch, CASL will do, provided that it supports a loose specifications semantics (the descriptions need denote only specifications, not implementations of the mathematical types). The languages mainly differ in the way in their organize specifications in the large, i.e. how they support modularization, genericity, and subtyping; these questions are orthogonal to our present discussion; it suffices that the specification yields a well-defined (possibly existentially quantified) type $\mathcal{A}$ with corresponding axioms.

A (for the reasoning framework) more critical question is how to specify the *abstraction function* a which is necessary if we want to derive from the information about the abstract $a(x)$ (provided by a specification) also information on the concrete x (needed for a verification). A very pragmatic solution is the one (implicitly) suggested by the model functions of JML [255]: the programmer defines a concrete program function in the implementation language that composes the abstract object in terms of the operations specified on $\mathcal{A}$. The properties of a required for reasoning are provided by a pre/post-condition pair on $\mathcal{A}$; if the implementation of the function can be verified against this specification, the consistency of this specification is guaranteed.

Since f and a operate on elements of C, understanding f and a can be considerably aided by introducing a *type discipline* also on the concrete program types. The type system shall be kept simple but suffice to keep an expression $x+1$ (with uninterpreted symbol x) apart from the integer $x+1$ (where x is an integer variable) and also indicate the syntax of expressions accepted and generated by a program (i.e. it shall allow to describe a suitable tree grammar [227]). More sophisticated constraints can be handled in the tradition of PVS and the proposer's RISC ProofNavigator [268, 271] by subtype predicates which give rise to type-checking conditions verified by a reasoner supporting the type checker.

All in all, the *specification of a program function* f then consists (backed by a collection previously defined abstract data types, abstraction mappings, and high-level properties on these) correctness lemmas (see below), a type signature for f (describing the concrete types of the arguments and results), a frame condition (mentioning any global variables assignable by f), a precondition, a postcondition (describing the relationship of the prestate to the poststate if the function has returned normally), and optionally an exceptional postcondition (describing the relationship of the prestate to the poststate, if the function has raised an exception); for (mutually) recursively defined functions, also termination terms may be provided that denote values from a well-founded ordering that must decrease with every invocation. Such a specification itself is already subject to reasoning: is it well-typed, is it trivial (equivalent to true), satisfiable (not equivalent to false), is it implied by another specification, etc?

To relate this specification to the actual implementation of f, a corresponding *type checking and reasoning calculus* for the underlying implementation language has to be devised. Since many computer algebra languages have a rather similar value and execution semantics, we will devise first a core language that captures the essential objects and constructs of these lan-

guages at a lower level and define the framework with respect to this core language. Compared to imperative/object-oriented languages, this is somewhat simplified because the semantics of basic data-types is simpler (e.g. unbounded integers rather than machine numbers) and the pointer-semantics of structures plays a less dominant role (most programs do not destructively update their arguments). In a second step, we will provide a translation from some high-level language subset(s) to this core language such that concrete programs can be treated. Analogously to ESC/Java2, there may be multiple translations of a language depending on the level of accuracy that the programs shall be modeled (e.g. by unfolding those loops that are not equipped with invariants by the user). The outcome of the framework are ultimately conditions that are necessary (and potentially also sufficient) be make the method meets its specification.

As for actually proving these conditions, in real-world scenarios we have to deal with the *partial under-specification* of abstract types respectively of notions defined on these types (e.g. undefined predicates) such that proofs of conditions depending on the semantics of these notions are actually not possible. Such situations will be typically detected in the course of these proofs; rather than just stating that a proof fails, it may be better to state the assumptions under which it would succeed (e.g. $A(x, y) \Rightarrow B(y)$ for undefined predicate B) and let the user, provided that he asserts the correctness of these assumptions or simpler ones, annotate the specification of a method with the assumptions and thus allow the proofs to make use of them. In this fashion, (previously also made but then implicit) correctness assumptions are now explicit and represent obligations for further formalization and proof.

We will work on a *supporting tool* that type-checks a program with respect to its type signature and, if this check succeeds, generates correctness conditions for the pre-conditions and (based on interfaces to automatic provers such as the Theorema system as well as to interactive proving assistants such as the proposer's RISC ProofNavigator) attempts to prove them. Again, the goal here is primarily to find internal inconsistencies in the program, post-conditions are just used as *assumptions* for the proofs of the pre-conditions of the subsequently called methods. To improve the level of automation, appropriate proving strategies are investigated and incorporated into the prover; if a proof fails, the tool provides the developer in a nice format with the knowledge available at a method call whose pre-condition could not be verified and requires further treatment (by manual verification or addition of a corresponding correctness assumption to the method); only when internal consistency with respect to the specification (and associated assumptions) is achieved, also the later verification of the program's postcondition may be attempted.

To guide our work, we will work with some program fragments from the CASA system (implemented in Maple) of the proposer of DK11. These are re-specified/re-written to our specification language and a corresponding subset of the implementation language to yield explicitly specified and internally consistent programs. Thus also errors in the original implementation will be detected and thus the reliability of the application will be improved.

Work plan

The organization of the Ph.D. work is sketched in the following table:

Months	Description
1–12	Course work with focus on CA, CA software, logic, formal methods Study of specification languages Sample specifications of CA methods
13–15	*Visit of an international institution*
16–24	Research on specification formalism, semantics and reasoning framework
25–27	*Visit of an international institution*
28–34	Work on specification checking prototype Application to sample specifications
35–36	Writing of Ph.D. thesis

After an initial training period with emphasis on courses related to computer algebra, software, logic, and formal methods, the Ph.D. student will start the investigation of prior work in formal specification and, based on an initial sketch of the proposed framework, work on sample specifications of concrete CA methods as available in the CASA system. Work on the actual details of the specification formalism, semantics, and reasoning framework, will proceed in close collaboration with the proposer, whose work during that time will focus on the development of a suitable software environment for education in program reasoning based on his prior work on the RISC ProofNavigator; the results of the PhD work will fit into this environment.

During the period of the actual research, the student will spend about six months total time for visits at institutions whose work is related to the Ph.D. topic. RISC has suitable contacts to various institutions that pursue the integration of computer algebra and logic, e.g. the Centre for Interdisciplinary Research in Computational Algebra in St. Andrews directed by Steve Linton (together with Ursula Martin who is now at the Queen Mary University of London director of a former project on embedded verification techniques for computer algebra) or the SPI research team at LIP6, Universite Pierre et Marie Curie Paris, directed by Therese Hardin (leader of the Focal project).

DK11 Franz Winkler: Rational Parametric Algebraic Curves

Abstract

We propose to investigate rational parametric algebraic curves both with respect to to their mathematical and geometric properties and also with respect to their manipulation by symbolic computation software. Rational curves and surfaces play an important role in geometric design or the integration theory of algebraic functions, but recently they have also been successfully use in diophantine analysis, and for finding general solutions of differential equations. Although algorithms for rational algebraic curves are already migrating from special purpose software systems (such as the CASA system developed by the proposer's research group) into mainstream computer algebra systems like MAPLE, there is in our view a demand for implementation of modern methods on such curves.

Current State of Research

For many years we have worked on the problem of rational parametrization of algebraic curves and surfaces together with Rafael Sendra (Madrid); see [283], [284], [285], [286], [288], [289], [290], [291], [292], [293], [294]. Currently we are finishing a book project on the topic of rational algebraic curves [296], due to be published by Springer-Verlag in 2007. We have been particularly interested in a computer algebra approach to problems related to rational algebraic curves.

This means that we want to compute with the smallest possible field in which we can express such a parametrization. Of course the parametrization should also be proper, i.e. have lowest possible degrees in the rational functions of its components, and it should be polynomial and normal (i.e. a surjective mapping of the affine line to the curve) if possible.

Such rational curve parametrizations, and in particular our parametrization algorithms, play an important role in the integration of algebraic functions, in computer aided geometric design, in the solution of Diophantine equations (compare [297], [298]), or in the computation of rational general solutions of algebraic ordinary differential equations (compare [299]). Let us illustrate the applicability of rational parametrization for these problem areas.

Diophantine equations

Let n be a positive integer, and let $\mathcal{C}_n$ be the curve defined by the polynomial

$$f_n(x,y) = x3 - (n-1)x^2y - (n+2)xy2 - y3 - 2ny(x+y).$$

First we check that all the curves $\mathcal{C}_n$ are rational (in fact, they are irreducible cubics with a double point at the origin). These curves $\mathcal{C}_n$ can be rationally parametrized as

$$\mathcal{P}_n(t) = \left(\frac{2nt2 + 2nt}{t3 - (n-1)t2 - (n+2)t - 1}, \frac{2nt + 2n}{t3 - (n-1)t2 - (n+2)t - 1} \right).$$

Let $W(n,t,s)$ be the homogenized (with homogenizing variable s) version of the denominator in this parametrization, and let $\mathcal{P}_n^*(t,s)$ be the homogenized version of the parametrization $\mathcal{P}_n$. We determine the integer solutions (t,s), with $\gcd(t,s) = 1$ and $t \geq 0$, of the Thue equations $W(n,t,s) = k$, where k divides $2n$. As the solution set we get

$$\mathcal{S} = \{(1,0),(0,1),(1,-1),(1,1),(1,-2),(2,-1),(1,-n-1),(n,1),(n+1,-n)\}.$$

Now $(0,0)$, the only integer singular point of $\mathcal{C}$, together with the points in

$$\{\mathcal{P}_n^*(t,s) \mid (t,s) \in \mathcal{S}\} \cap \mathbb{Z}2 = \{(0,0) = \mathcal{P}_n^*(1,0),\ \ (0,-2n) = \mathcal{P}_n^*(0,1)\}$$

are the integer solutions of the Diophantine equation $f_n(x,y) = 0$.
General solution of first order ordinary differential equations
Let us consider the differential equation

$$\begin{aligned} F(y,y') \ &= \ 229 - 144y + 16y(y')2 + 16y4 - 128y2 + 4y(y')3 + 4y3 \\ &\quad -4y3(y')2 - y2(y')2 + 6(y')2 + (y')3 + (y')4 \ = \ 0. \end{aligned}$$

The curve $\mathcal{C}$ associated to the differential equation is defined by the polynomial

$F(y,y_1) \ =$
$229 - 144y + 16yy_12 + 16y4 - 128y2 + 4yy_13 + 4y3 - 4y3y_12 - y2y_12 + 6y_12 + y_13 + y_14$.

We check that $\mathcal{C}$ is rational and we determine the rational parametrization

$$(r(x), s(x)) := \left(\frac{x3 + x4 + 1}{x2}, \frac{x3 + 2x4 - 2}{x} \right)$$

of $\mathcal{C}$. The differential equation $F(y,y')$ has a rational solution if and only if one of the following relations

$$ar'(x) = s(x) \quad \text{or} \quad a(x-b)^2 r'(x) = s(x), \qquad (*)$$

is satisfied, where $a, b \in \overline{\mathbb{Q}}$, and $a \neq 0$. Now, we see that

$$\frac{s}{r'} = x2.$$

Therefore, the second condition in $(*)$ is satisfied with $a = 1, b = 0$. Substituting

$$\frac{ab(x+c) - 1}{a(x+c)} = \frac{-1}{x+c},$$

in $r(x)$ we get the following rational general solution of the differential equation:

$$\hat{y} = \frac{-x - c + 1 + x4 + 4x^3 c + 6x^2 c2 + 4xc3 + c4}{(x+c)2}.$$

Software system CASA Since 1991 we have been implementing new algorithms for algebraic curves and surfaces in our software system CASA, based on the Maple computer algebra system (compare [282], [287], [295]). In the package "Algebraic Curves" of Maple 10, CASA is cited as a source of additional code on algebraic curves. Recently CASA has been listed in ORMS, the Oberwolfach References on Mathematical Software.

Objectives and Methods

As a thesis topic in this area we propose the systematic investigation of applications of parametrizations in computer aided geometric design, Diophantine analysis, differential equations, etc. As pointed out above, various researchers have found novel and interesting applications. But these applications can probably be extended and new applications can be developed. We are in close contact to Prof. Poulakis' research group in Thessaloniki for extending the applicability of parametrizations in Diophantine analysis. The application of parametrization to the solution of differential equations can possibly be extended to higher order equations or systems of such equations. Investigations in this area would fit very well into the other research area of the proposer's research group, namely the symbolic algebraic treatment of differential operators. Cooperation with the research groups of Bert Jüttler and Josef Schicho are intended.

The algorithmic techniques developed over the last decade, in particular the algorithms presented in [296], should be made available to the broader mathematical community. In particular we mean algorithms for the computation of the genus of an algebraic curve, various different approaches to the rational parametrization of curves, the minimization of the field extension in such a parametrization, rational optimal reparametrizations, and the determination of normal parametrizations. So we also want to emphasize the development and improvement of mathematical software. This means the redesign of the program system CASA. Currently CASA is implemented for an outdated version of Maple. The system would benefit from a completely new design of data structures, structuring of the code, and implementation in the latest version of Maple. Also, we need test suites for automatic updating to new versions of Maple. This thesis project could benefit from a close cooperation with the research group of Wolfgang Schreiner.

Work plan

The work on this PhD thesis is structured in the following way:

month	PhD work
1–12	course work focussed on commutative algebra and algebraic geometry, and symbolic computation software
13–18	beginning research work
19–24	the student should spend 1 semester at an other research institution
25–30	work on the mathematical and computer science aspects of the thesis, presentation of results at scientific meetings and partner institutions
31–36	writing of PhD thesis and final examination

DK12 Walter Zulehner: Efficient Solvers for KKT Systems

Abstract

KKT systems are special indefinite linear systems of equations with a natural block 2-by-2 structure. Of particular interest in this project are KKT systems that result from the discretization of constrained optimization problems in function spaces, like optimal design problems or optimal control problems, and from the discretization of mixed variational problems for systems of partial differential equations.

The focus in this project is the construction and analysis of efficient iterative methods for solving such systems, based on symmetric indefinite preconditioners. For these methods better properties are anticipated than for the better-understood block triangular preconditioners, if applied to problems with a (1,1) block which is only semi-definite, a property frequently occuring in KKT systems.

Current State of Research

We consider linear systems of equations in saddle point form

$$\begin{pmatrix} A & B^T \\ B & -C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} f \\ g \end{pmatrix}$$

with symmetric and positive semi-definite matrices A and C. Such block 2-by-2 systems can be interpreted as the first order optimality conditions (or Karush-Kuhn-Tucker conditions, KKT conditions) for a quadratic programming problem with linear equality constraints or for a corresponding penalized unconstrained quadratic programming problem. In this context, such a system is often called a KKT system.

In particular, we focus on large-scale sparse systems of this form, which arise by discretizing linear mixed variational problems for (systems of) partial differential equations (PDEs), or by discretizing the KKT conditions for linearly constrained (or penalized unconstrained) quadratic optimization problems in function spaces involving PDEs, like optimal design problems, optimal control problems and others. Linear systems in saddle point form also arise in nonlinearly constrained optimization (sequential quadratic programming and interior point methods).

For solving KKT systems with a PDE background iterative methods are considered to be superior to (sparse) direct methods, at least in the three-dimensional case. However, KKT systems are indefinite and require special care for constructing and analyzing iterative methods. Efficient iterative methods rely on good preconditioners and appropriate acceleration techniques (Krylov subspace methods).

Most of the solvers were constructed and analyzed under the standard assumption that

$$A \text{ is positive definite.}$$

Typical classes of preconditioners which rely on this standard assumption are block diagonal preconditioners, see, e.g., Rusten and Winther [333], Silvester and Wathen [336], block triangular preconditioners (originating from the classical Uzawa method [302]), see, e.g., Elman, Golub [319], Bramble, Pasciak, Vassilev [313], symmetric indefinite preconditioners, see, e.g., Dyn, Ferguson [318], Bank, Welfert, Yserentant [303], Rozložník, Simoncini [332], Al-Jeiroudi,

Gondzio, Hall [300], Dollar [315], and symmetric positive definite (but not block diagonal) preconditioners, see Vassilevski, Lazarov [342].

The preconditioners discussed so far obey the block 2-by-2 structure of the system and rely on good preconditioners for reduced systems in x and in y. As long as PDEs are involved multigrid techniques are available for constructing these preconditioners for the reduced systems. An alternative is to apply multigrid techniques directly to the whole system, which can also be viewed as a preconditioner. Here the construction and the analysis of the smoother is a main challenge. See, for example, Brandt, Dinar [314], Vanka [341], Wittum [345], Braess, Sarazin [311].

Depending on the properties of the preconditioned systems Krylov subspace methods either for symmetric indefinite or for non-symmetric systems like MINRES, BiCGStab, or GMRES were proposed. In Bramble, Pasciak [312] a block triangular preconditioner was used in order to obtain a preconditioned system which is symmetric and positive definite and, therefore, can be solved by the conjugate gradient method (CG), which is usually considered as the best or at least the best-understood Krylov subspace method. The block triangular preconditioner in [312] requires a symmetric and positive definite approximation $\hat{A}$ with $A - \hat{A}$ positive definite. In [332] an interesting equivalence between the right preconditioned simplified BiCGStab and a preconditioned conjugate gradient method (PCG) was obtained for the proposed indefinite preconditioner for a particular choice of the residuals. Yet another strategy to use CG was discussed, e.g., in Fischer, Ramage, Silvester, Wathen [320] and in Benzi, Simoncini [307], where the saddle point problem was reformulated by multiplying the second block row by -1 leading to a positive stable but non-symmetric system matrix.

See Benzi, Golub and Liesen [306] for a recent and extensive survey with more than 500 references most of them based on the standard assumptions.

Own contributions: In [347] a general approach for the analysis was presented for two classes of preconditioners: block triangular preconditioners and symmetric indefinite preconditioners. For acceleration CG methods were proposed and analyzed, extending the classical work by Bramble and Pasciak [312]. Multigrid preconditioners were analyzed and applied to the Stokes problem in [346] and [334]. The next two articles contain results from the PhD thesis of Markus Wabro, supervised by the proposer: In [343] and in [344] algebraic multigrid methods for the Oseen equations were presented and discussed. Multigrid preconditioners have been successfully applied to topology optimization problems in [338], [339] within the SFB-project F1309.

Interesting classes of problems, like certain problems in optimal control, lead to linear systems, where (in a stable sense)

$$A \text{ is positive definite only on the kernel of } B.$$

Much less is known in this case. One strategy is an augmented Lagrangian approach, where the matrix A and the vector f are replaced by a matrix of the form $A_W = A + B^T W B$ and a vector $f_W = f + B^T W g$, respectively, with an appropriate matrix W, see e.g. Fortin and Glowinski [321]. This does not change the solution of the problem, and the new (1,1) block A_W becomes positive definite if W is properly chosen, e.g, if it is positive definite, and all methods working under the standard assumption applied to the augmented system could be used, in principle. It is, however, a delicate issue to choose the matrix W in order to obtain good convergence properties, see the discussions in Golub and Greif [324], Golub, Greif and Varah [325].

Another approach is offered by a particular class of symmetric indefinite preconditioners, the so-called constraint preconditioners, see, e.g., Keller, Gould, Wathen [329], Gould, Hribar, Nocedal [326], Dollar, Gould, Schilders, Wathen [316]. These preconditioners are not restricted to the case of positive definite matrices A. For this class of preconditioners (projected) PCG was successfully used as acceleration technique. One possible drawback of this class of preconditioners is the computational costs involved in the application of the preconditioner, where in some way or another some projection onto $\ker B$ has to be realized.

Preconditioners specially tailored to PDE-constrained optimization problems, where A is typically only positive definite on the kernel of B, were proposed, for example, by Hackbusch [327], Ta'asan [340], Arian, Ta'asan [301], Battermann, Heinkenschloss [304], Battermann, Sachs [305], Biros, Ghattas [308], [309], Hazra, Schulz [328], Dreyer, Marr, Schulz [317], Borzi, Kunisch, Kwak [310].

Own contributions: The analysis of symmetric indefinite preconditioners was extended and applied to a problem from optimal control in [335]. Multigrid preconditioners were analyzed and applied to an optimal control problem in [337].

For certain classes of KKT systems a richer

$$\text{block } n\text{-by-}n \text{ structure with } n > 2$$

can be identified and exploited, see [322] and [323].

Own contributions: In [348] block triangular preconditioners were analyzed. Such preconditioners were successfully applied to the so-called BETI method for second-order elliptic boundary value problems, see [330], [331].

Objectives and Methods

Block triangular preconditioners are well investigated in literature. Properly scaled they can be used in combination with the CG method, usually considered as the best Krylov subspace method. An extension from a block 2-by-2 system to an block n-by-n system is available.

However, usually the construction and analysis of block triangular preconditioners are based on the assumption of a positive definite matrix A, or, more generally, a positive definite (1,1) block of the KKT system, which excludes its direct application to interesting classes of optimization problems. And the scaling for $n > 2$ is computationally rather costly.

The first drawback is not necessarily shared by symmetric indefinite preconditioners as it was demonstrated in [335] for $n = 2$. Therefore, we will concentrate on symmetric indefinite preconditioners in this project.

A proper scaling guarantees the application of the CG method, however, may deteriorate the quality of the preconditioner. On the other hand, without scaling the symmetry and positive definiteness and, therefore, the application of the CG method is no longer guaranteed, the preconditioned matrix remains only positive real, for which Krylov subspace methods like QMR are appropriate acceleration techniques. So a first objective is thorough analysis of the behavior of symmetric indefinite preconditioners if no special scaling is used and a comparison with the scaled approach, starting from the work in [347] and considering the completely different approaches in [332], [320] and [307].

A second objective is to extended the construction and analysis of symmetric and indefinite preconditioners to problems with a richer block n-by-n structure. The approach taken in [348]

in combination with the ideas from [335] should provide a guideline for these investigations. It is expected that the scaling is easier to handle for $n > 2$ compared to block triangular preconditioners.

The analysis of the preconditioners is typically based on assumptions of available preconditions for reduced systems (for $n = 2$ reduced systems in x and in y). The particular choice of these preconditioners depend on the available information for selected classes of KKT systems. So a third general objective is to identify interesting classes of KKT systems, where such information is available. Of particular interest for the construction is the robustness of the methods from discretization parameters and/or other parameters like regularization parameters. Concerning regularization parameters a first step is set in [335], which could be the starting point for similar strategies for other classes of problems.

1.2 Additionality

In the frame of the SFB we have started our initiative to combine two disciplines of computational mathematics, numerical analysis and symbolic computation, which have been considered as "two different worlds" so far. The scientific basis of this enterprise was given by the expertise accumulated in the numerical and symbolic research groups at the Johannes Kepler University. Encouraged by the results of interdisciplinary SFB research (i.e., non-trivial interaction of numerical and symbolic methods), we felt that this new type of interdisciplinarity should be supported by adequate educational measures.

As a consequence, some of these ideas entered even the JKU Master Curriculum in "Technical Mathematics." For example, a new special course "Algorithmic Methods" has been introduced that accompanies the standard "big" introductory lectures on linear algebra and analysis during the first two semesters. The novelty of the "Algorithmic Methods" course consists not only in bringing in computational aspects at the bachelor stage of training, but also in presenting numerical and symbolic procedures just as two "different sides of the same coin", namely, of algorithmic mathematics. A corresponding text book (bachelor level) is in preparation. The "numerical" author, Ph. Kügler, is member of the JKU Institute for Industrial Mathematics, the "symbolic" author, W. Windsteiger, is member of RISC.

The proposed DK will provide such a training on the graduate level. The long-term goal is to establish a distinguished PhD Program at JKU which will attract young researchers from all over the world.

1.3 Training goals

Already for the first period, the overall goal of the DK program will be to provide intensive PhD training in two fundamental areas of computational mathematics: numerical analysis (in particular, of direct and inverse field problems) and symbolic computation. This will be accomplished by course work that involves lectures from both areas and by interdisciplinary seminars; see Section 1.4 below.

Such kind of DK education will stimulate numerous new avenues of research. For example: DK graduates will be able to develop new solvers to direct or inverse problems by combining numerical approaches with symbolic methods like Groebner bases; DK graduates will design new procedures for geometrical scientific computing by utilizing implementations of computer algebra algorithms for problems in algebraic geometry; DK graduates will use symbolic special function algorithms to speed-up hp finite element methods; DK graduates will use symbolic optimization techniques for constructing new algebraic multilevel preconditioners, etc. — It should be noted that first results in each of these directions have been already achieved within the SFB. So the DK will benefit from SFB experience about how to establish necessary interdisciplinary interaction.

General aspects of the qualification profile of DK graduates are:

- A DK graduate has produced a PhD thesis in an up-to-date subarea of computational mathematics.
- A DK graduate is expert in algorithmic mathematics; he/she is able to combine the "two worlds" of numerical and symbolic methods.

- A DK graduate has got extra training to develop skills concerning general aspects of mathematical problem solving, the presentation (written and oral) of mathematical work (also to a non-mathematical audience), programming, and how to work in groups embedded in an international research network.

- A DK graduate is experienced in aspects of scientific management. — In order to achieve this training effect, the DK will encourage the DK students to participate actively in the organization of workshops and conferences, and in many other aspects of scientific life.

- A DK graduate is qualified to pursue a professional career either in academia or in industry.

1.4 DK-specific training goals

For each DK collegiate an *individual* curriculum will be compiled. It consists of a selection of courses that fit best to the PhD topic chosen.

Course work. The total amount of course work during the 3 years of DK study will be equivalent to 12 one-semester courses, 2 hours per week each. Special emphasis is put on selecting courses in such a way that a good balance between numerics and symbolics is achieved.

Only 2 one-semester courses (2 hours per week each), especially designed for the DK, will be mandatory for all the DK students. In "Fundamentals of Numerical and Symbolic Computation" DK scientists from numerics and symbolics will present case studies in order to introduce to basic notions and methods of general relevance to the DK. In "Thinking-Speaking-Writing" DK students will be actively trained in mastering practical aspects of scientific work: problem solving strategies and how to present mathematical work in written or oral form. (This course, introduced by Buchberger, has been a key ingredient in the RISC PhD Curriculum for about 20 years.) — Most of the other DK courses will be selected from the standard mathematics curriculum at the Johannes Kepler University, e.g.: Automated Theorem Proving, Computational Linear Algebra, Computational Logic, Computer Aided Geometric Design, Computer Algebra, Computer Analysis, Differential Geometry, Formal Methods in Software Development, Functional Programming, Inverse and Ill-Posed Problems, Numerical Methods for Elliptic Equations, Special Functions, Symbolic Analysis (operator methods), or Symbolic Summation, It should be mentioned that some of these lectures, like Computational Linear Algebra, Special Functions or Symbolic Analysis, have emerged from SFB research cooperations.

In case that DK topics need to be covered by new courses, such courses will be offered. For instance, for the first DK period we plan to introduce courses on: Computational Geometry, Boundary Element Methods, or Introduction to Learning Theory. The JKU considers the official integration of such specific DK lectures into the JKU mathematics curriculum with special priority.

Seminars. In addition to course work, each DK student has to participate actively in a weekly (2 hours) seminar. Typically these are DK topic oriented, special project seminars regularly run by the DK advisors. Often such seminars will be jointly organized by several DK project leaders.

For thesis projects with particulary strong interdisciplinary interaction, joint seminars involving the respective DK research groups will be organized.

Advisorship. Besides participating in weekly seminars, each DK student will have a regular individual meeting with his/her advisor(s) at least once a week.

At a certain stage of a DK thesis project, one or two co-advisors (DK scientists) will be chosen depending on the scientific background of the project. DK theses of particularly strong interdisciplinary character will be co-advised by experts from different areas.

If a DK thesis is evolving in close cooperation with an external research group, a co-advisor can be chosen from this group.

DK Report Day. At the end of each semester there will be a "report-day" where the DK students — in the presence of all the DK scientists — will report on the progress of their thesis work.

DK Visitors Program. In the DK, special emphasis is put on international contacts and collaborations. Within the frame of a *DK Visitors Program*, national and international research partners will be invited for short or long term research stays at the DK. DK students will benefit from courses and guest lectures presented by invited DK guest professors and researchers. — Concerning "outgoing" activities of DK students, see Section 1.5.

DK Colloquium. Once a month a *DK Colloquium Talk* will be organized. Typically these are survey talks presented by guests invited in the frame of the DK Visitors Program.

1.5 Stays abroad

We recommend our DK students to spend in average about 6 months at other other research institutions in Austria or abroad, if it is of meaningful for their DK projects.

The stays abroad can be partitioned into short or long term research visits. But the total time period spent abroad should be 4 to 8 month for each DK student.

2 Appendix

2.1 List of citations in project descriptions

This section contains the references of the citations given in the particular DK thesis project descriptions of Section 1.1.4. The references are grouped as follows: for each DK project the corresponding references can be found in a separate list.

References DK Buchberger

[1] J. Apel. *Gröbner Basen in Nichtkommutativen Algebren und ihre Anwendung.* (*Gröbner Bases in Noncommutative Algebras and their Application.*) PhD Thesis, Institute of Mathematics, University of Leipzig, Germany, 1988.

[2] G. Bergman. *The Diamond Lemma for Ring Theory.* Adv. Math., Vol. 29/2, pp. 178–218, 1978.

[3] B. Buchberger, A. Craciun, T. Jebelean, L. Kovacs, T. Kutsia, K. Nakagawa, F. Piroi, N. Popov, J. Robu, M. Rosenkranz, W. Windsteiger. *Theorema: Towards Computer-Aided Mathematical Theory Exploration.* Journal of Applied Logic, Vol. 4/3, Special Issue "Towards Computer-Aided Mathematic", (C. Benzmüller ed.), pp. 470–504, December 2006.

[4] B. Buchberger. *Algorithm Supported Mathematical Theory Exploration: A Personal View and Strategy.* In: Proceeding of 7th International Conference on Artificial Intelligence and Symbolic Computation, September 22-24, 2004, RISC, Johannes Kepler University, Austria, Springer Lecture Notes in Artificial Intelligence, Vol. 3249, Springer, Berlin, Heidelberg, pp. 236–250, 2004.

[5] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem Nulldimensionalen Polynomideal.* PhD Thesis, Institute of Mathematics, University of Innsbruck, Austria, 1965. English translation: *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal.* Journal of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. Vol. 41/3-4, pp. 475–511, 2006.

[6] B. Buchberger. *Ein Algorithmisches Kriterium für die Lösbarkeit eines Algebraischen Gleichungssystems.* Aequationes mathematicae Vol. 4/3, 1970, pp. 374–383. English translation: *An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations.* In: [7], pp. 535–545.

[7] B. Buchberger, F. Winkler (eds.). *Gröbner Bases and Applications.* Proceedings of the International Conference "33 Years of Gröbner Bases", 1998, Research Institute for Symbolic Computation, Johannes Kepler University, Austria. London Mathematical Society Lecture Note Series, Vol. 251, Cambridge University Press, 1998.

[8] B. Buchberger. *An Introduction to Gröbner Bases.* Talk at University of Genova, Mathematical Department, July 1983.

[9] B. Buchberger. *Proving by First and Intermediate Principles.* Invited talk at the Workshop on Types for Mathematics / Libraries of Formal Mathematics, University of Nijmegen, November 1-2, 2004. Download talk 2004-11-01-A on `http://www.risc.uni-linz.ac.at/people/buchberg/invitedconf_talks.php`.

[10] M. Giese, B. Buchberger. *Toward Practical Reflection for Formal Mathematics.* Technical Report, RISC (Research Institute for Symbolic Computation), Johannes Kepler University, Linz, Austria, April 2007. Download paper 2007-04-10-A on `http://www.risc.uni-linz.ac.at/people/buchberg/unrefereed_publications.php`

[11] B. Buchberger. *Mathematica as a Rewrite Language.* In: Functional and Logic Programming, Proceedings of the 2nd Fuji International Workshop on Functional and Logic Programming, November 1-4, 1996, Shonan Village Center, T. Ida, A. Ohori, M. Takeichi (eds.), World Scientific, Singapore - New Jersey - London - Hong Kong, pp. 1–13, 1996. Download paper 1996-11-01-A on `http://www.risc.uni-linz.ac.at/people/buchberg/refereed_publications.php`

[12] B. Buchberger. *Gröbner Rings in Theorema: A Case Study in Functors and Categories.* Technical Report no. 2003-49, Johannes Kepler University Linz, Spezialforschungsbereich F013, November 2003. Download paper 2003-11-00-A on `http://www.risc.uni-linz.ac.at/people/buchberg/unrefereed_publications.php`

[13] J. Bueso, J. Gomez-Torrecillas, A. Verschoren. *Algorithmic Methods in Noncommutative Algebra: Applications to Quantum Groups.* Springer, ISBN 978-1402014024, 2003.

[14] E. Green. *An Introduction to Noncommutative Gröbner Bases.* In: K.G. Fisher (ed.), Computational Algebra, Lecture Notes on Pure and Applied Mathematics, Vol. 151, Dekker, New York, pp. 167–190, 1994.

[15] F. Chyzak. *Gröbner Bases, Symbolic Summation and Symbolic Integration.* In: [7], pp. 32–60.

[16] F. Chyzak, P. Paule. *Computer Algebra.* In: D. Lozier, editor, NIST's Digital Library of Mathematical Functions, DLMF, 2008. In preparation.

[17] F. Chyzak, A. Quadrat, D. Robertz. *Effective Algorithms for Parametrizing Linear Control Systems Over Ore Algebras.* Applicable Algebra in Engineering, Communications and Computing, Vol. 16/5, pp. 319–376, November 2005.

[18] F. Chyzak. *An Extension of Zeilberger's Fast Algorithm to General Holonomic Functions.* Discrete Mathematics, Vol. 217, pp. 115–134, 2000.

[19] P. Ackermann, M. Kreuzer. *Gröbner Basis Cryptosystems.* Journal Appl. Alg., Vol. 17, pp. 173–194, 2006.

[20] W. Diffie, M.E. Hellman. *New Directions in Cryptography.* In: IEEE Transactions on Information Theory, IT–22(6), pp. 644–654, 1976.

[21] T. Matsumoto, H. Imai. *Public Quadratic Polynomial-Tuples for Efficient Signature Verification and Message Encryption.* In: Advances in Cryptology – EUROCRYPT 1988, LNCS, Vol. 330, Springer–Verlag, pp. 419–453, 1988.

[22] J.C. Faugère. *A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero F5.* In: T. Mora (ed.), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC) 2002, ACM Press, pp. 75–83, July 2002.

[23] G.-M. Greuel, G. Pfister. *A Singular Introduction to Commutative Algebra.* Springer, ISBN 3-540-42897-6, 2002.

[24] A.I. Shirshov. *Some Algorithmic Problems for Lie Algebras* (Russian). Sib. Mat. Zh., Vol 3, pp. 292–296, 1962.

[25] R. Loos. *Generalized Polynomial Remainder Sequences.* In: B. Buchberger, G. E. Collins, and R. Loos (eds.), Computer Algebra: Symbolic and Algebraic Computation, Springer, Vienna - NY, pp. 115–137, 1982.

[26] A. Mandache. *Gröbner Bases Computation and Gaussian Elimination.* PhD Thesis, Research Institute for Symbolic Computation, Univ. of Linz, Austria, 1995.

[27] M.Kaufmann, P. Manolios, J.S. Moore (eds.). *Computer-Aided Reasoning: ACL2 Case Studies.* Kluwer Academic Publishers, June, 2000.

[28] P. Rudnicki, A. Trybulec. *On the Integrity of a Repository of Formal Mathematics.* In: A. Asperti, B. Buchberger, J.H. Davenport(eds.), Proceedings of MKM-2003, Springer, LNCS, Vol. 2594, pp. 162–174, 2003.

[29] J. Patarin. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP).* In: Two New Families of Asymmetric Algorithms. Proc. EUROCRYPT '96, LNCS, Vol. 1070, Springer, pp. 33–48, 1996.

[30] M. Giesbrecht, E. Kaltofen et al. *Project LinBox: Exact Computational Linear Algebra.* Homepage: `http://www.linalg.org/index.html`

[31] A. Kandri-Rody, V. Weispfenning. *Noncommutative Gröbner Bases in Algebras of Solvable Type.* Journal of Symbolic Computation, Vol. 9/1, pp. 1–26, 1987.

[32] Y. Kobayashi. *Gröbner Bases of Associative Algebras and the Hochschild Cohomology.* Trans. Am. Math. Soc., Vol. 357, pp. 1095-1124, 2004.

[33] D. E. Knuth, P. B. Bendix. *Simple Word Problems in Universal Algebra.* In: J. Leech (ed.), Computational Problems in Abstract Algebra, Pergamon Press, pp. 263–297, 1970.

[34] V. Levandovskyy. *Noncommutative Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications, and Implementation.* PhD Thesis, Department of Mathematics, University of Kaiserlautern, Germany, 2005.

[35] V. Levandovskyy. *A Comparison of Systems for Gröbner Bases.* Online list compiled in the frame of the Special Semester on Gröbner Bases, organized by Radon Institute for Computational and Applied Mathematics (Austrian Academy of Science) and Research Institute for Symbolic Computation (RISC), directed by B. Buchberger, see `http://www.ricam.oeaw.ac.at/specsem/srs/groeb/` (link "Groebner Basis Implementations").

[36] F.J. Lobillo, C. Rabelo. *A SINGULAR 3.0 Library for Computations with Quantum Matrices, Quantum Minors and Symmetric Groups.* Singualar 3.0 Documentation, Math. Institute, University of Kaiserlautern, Germany, 2004.

[37] T. Mora. *Gröbner Bases for Noncommutative Polynomial Rings.* In: Proceedings of AAECC-3 (J. Calmet ed.), LNCS, Vol. 229, pp. 353–363, 1986.

[38] D. Zeilberger. *A Holonomic Systems Approach to Special Function Identities.* Journal of Computational and Applied Mathematics, Vol. 32, pp. 321–368, 1990.

[39] N. Takayama. *An Algorithm of Constructing the Integral of a Module.* In: Proceedings of ISSAC'90, pp. 206–211, 1990.

[40] N. Takayama. *Gröbner Basis, Integration and Transcendental Functions.* In: Proceedings of ISSAC'90, pp. 152–156, 1990.

[41] F. Chyzak, B. Salvy. *Noncommutative Elimination in Ore Algebras Proves Multivariate Identities.* Journal of Symbolic Computation, Vol. 26, pp. 187–227, 1998.

[42] M. Rosenkranz, B. Buchberger, H.W. Engl. *Solving Linear Boundary Value Problems Via Noncommutative Groebner Bases.* Applicable Analysis, Vol.82/7, pp. 655–675, July 2003.

[43] M. Rosenkranz. *The Green's Algebra: A Polynomial Approach to Boundary Value Problems.* Ph.D. Thesis, University of Linz, Austria, 2003.

[44] M. Rosenkranz. *New Symbolic Method for Solving Linear Two-Point Boundary Value Problems on the Level of Operators.* Journal of Symbolic Computation, Vol. 39, pp. 171–199, 2005.

[45] M. Rosenkranz, G. Regensburger. *Solving and Factoring Boundary Problems for Linear Ordinary Differential Equations in Differential Algebras.* Technical Report, 2007-8, Johannes Kepler University Linz, Spezialforschungsbereich F013, November 2007.

[46] W. Habicht. *Zur Inhomogenen Eliminationstheorie.* Commentarii Mathematici Helvetici, Vol. 21/1, pp. 79–98, 1948.

[47] M. Kreuzer, L. Robbiano. *Computational Commutative Algebra 1*, Springer, ISBN 3-540-67733-X, 2000.

[48] A. Zapletal, B. Buchberger. *Online Bibliography on Gröbner Bases.* Compiled in the frame of the Special Semester on Gröbner bases 2006 directed by B. Buchberger. `http://www.ricam.oeaw.ac.at/Groebner-Bases-Bibliography/`

[49] T.S. Rai. *Infinite Gröbner Bases and Noncommutative Polly Cracker Cryptosystems.* PhD Thesis, Virginia Polytechnique Institute and State Univ., 2004.

[50] V. Ufnarovski. *Introduction to Noncommutative Gröbner Bases Theory.* In: [7], pp. 259–280.

References DK Jüttler

[51] M. Bartoň. *Bernstein–Bézier techniques for computing roots of polynomials and of polynomial systems.* PhD thesis, Charles University, Faculty of Mathematics and Physics, Prague, 2007. co–supervised by A. Karger and B. Jüttler.

[52] M. Bartoň and B. Jüttler. Computing roots of polynomials by quadratic clipping. *Comp. Aided Geom. Design*, 24:125–141, 2007.

[53] G. Elber and M.-S. Kim. Geometric constraint solver using multivariate rational spline functions. In *The Sixth ACM/IEEE Symposium on Solid Modeling and Applications*, pages 1–10, Ann Arbor, MI, 2001.

[54] G. Farin, J. Hoschek, and M.-S. Kim, editors. *Handbook of computer aided geometric design.* North-Holland, Amsterdam, 2002.

[55] R.T. Farouki and T.N.T. Goodman. On the optimal stability of the Bernstein basis. *Math. Comp.*, 65:1553–1566, 1996.

[56] J. Garloff, C. Jansson, and A.P. Smith. Lower bound functions for polynomials. *J. Comput. Appl. Math.*, 157:207–225, 2003.

[57] J. Garloff and A. P. Smith. Solution of systems of polynomial equations by using Bernstein expansion. Alefeld, Götz (ed.) et al., Symbolic algebraic methods and verification methods. Wien: Springer. 87-97 (2001).

[58] L. Gonzalez-Vega and I. Necula. Efficient topology determination of implicitly defined algebraic plane curves. *Comput. Aided Geom. Design*, 19:719–743, 2002.

[59] H.-S. Heo, S. J. Hong, M.-S. Kim, and G. Elber. The intersection of two ringed surfaces and some related problems. *Graphical Models*, 63(4):228–244, 2001.

[60] A. Hofinger and J Valdman. Numerical solution of the two-yield elastoplastic minimization problem. Technical Report 18, Johannes Kepler University Linz, SFB F013, 2006. `www.sfb013.uni-linz.ac.at`.

[61] M.L. Husty, M. Pfurner, and H.-P. Schröcker. A new and efficient algorithm for the inverse kinematics of a general serial $6R$ manipulator. *Mech. Mach. Theory*, 42:66–81, 2007.

[62] A. Kayumov and M.-L. Mazure. Chebyshevian splines: interpolation and blossoms. *C. R., Math., Acad. Sci. Paris*, 344:65–70, 2007.

[63] K. Lee. *Principles of CAD/CAM/CAE systems.* Addison-Wesley, 1999.

[64] T.Y. Li. Numerical solution of polynomial systems by homotopy continuation methods. In F. Cucker, editor, *Special Volume: Foundations of Computational Mathematics*, volume XI of *Handbook of Numerical Analysis*, pages 209–304. North–Holland, 2003.

[65] D. Lutterkort and J. Peters. Optimized refinable enclosures of multivariate polynomial pieces. *Comput. Aided Geom. Design*, 18:851–863, 2001.

[66] E. Mainar and J.M. Peña. Evaluation algorithms for multivariate polynomials in Bernstein-Bézier form. *J. Approximation Theory*, 143:44–61, 2006.

[67] J.M. McNamee. Bibliographies on roots of polynomials. *J. Comp. Appl. Math.*, 47:391–394, 78:1–1, 110:305–306, 142:433–434, 1993–2002.

[68] B. Mourrain and J.-P. Pavone. Subdivision methods for solving polynomial equations. Technical Report 5658, INRIA Sophia Antipolis, 2005.

[69] B. Mourrain, F. Rouillier, and M.-F. Roy. The Bernstein-basis and real root isolation. Goodman, Jacob Eli (ed.) et al., Combinatorial and computational geometry. Cambridge University Press. 459-478 (2005).

[70] A. Neumaier. *Interval methods for systems of equations.* Cambridge University Press, 1990.

[71] T. Nishita, T.W. Sederberg, and M. Kakimoto. Ray tracing trimmed rational surface patches. In *Proc. Siggraph*, pages 337–345. ACM, 1990.

[72] N.M. Patrikalakis and T. Maekawa. *Shape interrogation for computer aided design and manufacturing.* Springer, Berlin, 2002.

[73] H. Prautzsch, W. Boehm, and M. Paluszny. *Bézier and B-spline techniques.* Springer, Berlin, 2002.

[74] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial's real roots. *J. Comput. Appl. Math.*, 162:33–50, 2004.

[75] S.M. Rump. Ten methods to bound multiple roots of polynomials. *J. Comput. Appl. Math.*, 156:403–432, 2003.

[76] E.C. Sherbrooke and N.M. Patrikalakis. Computation of the solutions of nonlinear polynomial systems. *Comp. Aided Geom. Design*, 10:379–405, 1993.

[77] A. J. Sommese and C. W. Wampler. *The numerical solution of systems of polynomials arising in engineering and science.* World Scientific, 2005.

References DK Langer

[78] S. Beuchler, T. Eibner, and U. Langer. Primal and dual interface concentrated iterative substructuring methods. RICAM-Report Nr. 2007-7, Johann Radon Institut for Computational and Applied Mathematics, 2007. and submitted.

[79] D. Braess. *Finite Elemente – Theorie, schnelle Löser und Anwendungen in der Elastizitätstheorie*. Springer–Lehrbuch. Springer Verlag, Berlin, Heidelberg, 1992.

[80] S.C. Brenner and L.R. Scott. *The Mathematical Theory of Finite Element Methods*. Springer-Verlag, New York, Berlin, heidelberg, 1994.

[81] F. Brezzi and M. Fortin. *Mixed and Hybrid Finite Element Methods*. Springer Series in Computational Mathematics. Springer–Verlag, Berlin, 1991.

[82] F. Brezzi, K. Lipnikov, and M. Shashkov. Convergence of mimetic finite difference method for diffusion problems on polyhedral meshes. *SIAM J. Num. Anal.*, 43(3):1872–1896, 2005.

[83] C. Carstensen, M. Kuhn, and U. Langer. Fast parallel solvers for symmetric boundary element domain decomposition equations. *Numer. Math.*, 79:321–347, 1998.

[84] M. Costabel. Symmetric methods for the coupling of finite elements and boundary elements. In C.A. Brebbia, W.L. Wendland, and G. Kuhn, editors, *Boundary Elements IX*, pages 411–420, Berlin, Heidelberg, New York, 1987. Springer.

[85] T. Eibner and J. M. Melenk. Multilevel preconditioning for the boundary concentrated hp-fem. *Comp. Meth. Mech. Eng.*, 2007. accepted.

[86] T. Eibner and J.M. Melenk. A local error analysis of the boundary-concentrated *hp*-FEM. *IMA J. Numer. Anal.*, 27(1):752–778, 2007.

[87] G. C. Hsiao and W. L. Wendland. Domain decomposition in boundary element methods. In *Proceedings of the Fourth International Symposium on Domain Decomposition Methods for Partial Differential Equations (ed. by R. Glowinski and Y.A. Kuznetsov and G. Meurant and J. Périaux and O. B. Widlund), Moscow, May 21-25, 1990*, pages 41–49, Philadelphia, 1991. SIAM.

[88] B.N. Khoromskij and J. M. Melenk. Boundary concentrated finite element methods. *SIAM J. Numer. Anal.*, 41(1):1–36, 2003.

[89] B.N. Khoromskij and J.M. Melenk. An efficient direct solver for the boundary concentrated FEM in 2D. *Computing*, 69:91–117, 2002.

[90] Y. Kuznetsov, K. Lipnikov, and M. Shashkov. Convergence of mimetic finite difference method for diffusion problems on polyhedral meshes. *Comp. Geosciences*, 8(4):301–324, 2004.

[91] U. Langer. Parallel iterative solution of symmetric coupled FE/BE- equations via domain decomposition. *Contemporary Mathematics*, 157:335–344, 1994.

[92] U. Langer, G. Of, O. Steinbach, and W. Zulehner. Inexact data-sparse boundary element tearing and interconnecting methods. *SIAM Journal on Scientific Computing*, 29(1):290–314, 2007.

[93] U. Langer and O. Steinbach. Boundary element tearing and interconnecting method. *Computing*, 71(3):205–228, 2003.

[94] U. Langer and O. Steinbach. Coupled finite and boundary element domain decomposition methods. In *In "Boundary Element Analysis: Mathematical Aspects and Application", ed. by M. Schanz and O. Steinbach, Lecture Notes in Applied and Computational Mechanic, Volume 29*, pages 29–59, Berlin, 2007. Springer.

[95] S. Sauter and C. Schwab. *Randelementemethoden: Analyse, Numerik und Implementierung schneller Algorithmen*. Teubner-Verlag, Stuttgart, Leipzig, Wiesbaden, 2004.

[96] O. Steinbach. *Numerische Näherungsverfahren für elliptische Randwert-probleme: Finite Elemente und Randelemente*. Teubner-Verlag, Stuttgart, Leipzig, Wiesbaden, 2003.

[97] A. Toselli and O. Widlund. *Domain Decoposition Methods – Algorithms and Theory*, volume 34 of *Springer Series in Computational Mathematics*. Springer, Berlin, Heidelberg, 2005.

[98] H. Yserentant. Coarse grid spaces for domains with a complicated boundary. *Numer. Algorithms*, 21(1-4):387–392, 1999.

References DK Paule

[99] http://www.risc.uni-linz.ac.at/research/combinat/

[100] F. Chyzak and P. Paule, *Computer Algebra*, 40 pages. To appear as a separate chapter in: The Digital Library of Mathematical Functions (DLMF), (F. Olver et al., eds.), National Institute of Standards and Technology (NIST),Gaithersburg, U.S.A., 2007.

[101] http://dlmf.nist.gov/

[102] M. Abramowitz and I. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Applied Mathematical Series 55, National Bureau of Standards, Washington, DC, 1964; reprinted: Dover, New York, 1965.

[103] E.D. Rainville, Special Functions. Macmillan, New York, 1960.

[104] D. Zeilberger, *A holonomic systems approach to special function identities*, J. Comput. Appl. Math. 32 (1990), 321–368.

[105] D. Zeilberger, *A fast algorithm for proving terminating hypergeometric identities*, Discrete Math. 80 (1990), 207–211.

[106] R.W. Gosper, *Decision procedures for indefinite hypergeometric summation*, Proc. Nat. Acad. Sci. U.S.A. 75 (1978), 40–42.

[107] H.S. Wilf and D. Zeilberger, *An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities*, Invent. Math. 108 (1992), 575–633.

[108] S.A. Abramov, *On the summation of rational functions*, USSR Comp. Maths. Math. Phys. 11 (1971), 324–330.

[109] M. Karr, *Summation in finite terms*, J. ACM 28 (1981), 305–350.

[110] C. Schneider, Symbolic Summation in Difference Fields. PhD Thesis, Technical Report 01-17, RISC, J. Kepler University, 2001.

[111] P. Paule, *Greatest factorial factorization and symbolic summation*, J. Symbolic Comput. 20 (1996), 235–268.

[112] M. Petkovšek, *Hypergeometric solutions of linear recurrences with polynomial coefficients*, J. Symb. Comput. 14 (1992), 243–264.

[113] B.Salvy and P. Zimmermann, *Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable*, ACM Trans. Math. Software 20 (1994), 163–177.

[114] N. Takayama, *An algorithm of constructing the integral of a module - an infinite dimensional analog of Gröbner basis*, in: Proc. ISSAC'090, Kyoto, ACM and Addison-Wesley, 1990.

[115] F. Chyzak. Fonctions holonomes en calcul formel. PhD thesis, École polytechnique, INRIA, TU 0531, 1998.

[116] R. Lyons, P. Paule, and A. Riese, *A computer proof of a series evaluation in terms of harmonic numbers*, Appl. Algebra Engrg. Comm. Comput. 13 (2002), 327–333.

[117] A. Bećirović, P. Paule, V. Pillwein, A. Riese, C. Schneider, and J. Schöberl, *Hypergeometric summation algorithms for high order finite elements*, Computing 78 (2006), 235–249.

[118] G.E. Andrews, P. Paule, and C. Schneider, *Plane partitions VI: Stembridge's TSPP theorem*, Adv. Appl. Math. 34 (2005), 709–739.

[119] C. Schneider, A new Sigma approach to multi-summation, Adv. Appl. Math. 34 (2005), 740–767.

[120] G.E. Collins, *Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition*, in: Lecture Notes in Computer Science 33 (1975), 134–183.

[121] S. Gerhold and M. Kauers, *A procedure for proving special function inequalities involving a discrete parameter*. In: Proceedings of ISSAC'05, ACM, 2005, 156–162.

[122] M. Kauers, *SumCracker — a package for manipulating symbolic sums and related objects*, Technical Report 2005-21, SFB F013, J. Kepler University, 2005.

[123] S. Gerhold and M. Kauers, *A computer proof of Turan's inequality*, J. Inequal. Pure Appl. Math. 7 (2006), Art. 42.

[124] P. Turan, *On the zeros of the polynomials of Legendre*, Časopis Pest. Mat. Fys. 75 (1950), 113–122.

[125] H. Alzer, S. Gerhold, M. Kauers, and A. Lupas, *On Turan's inequality for Legendre polynomials*, Expositiones Mathematicae, to appear 2007.

[126] V.H. Moll, *The evaluation of integrals: A personal story*, Notices of the AMS 49 (2002), 311–317.

[127] M. Kauers and P. Paule, *A computer proof of Moll's log-concavity conjecture*, SFB-Report No. 2006-15, 2006. (To appear in: Proceedings of the AMS.)

[128] K. Wegschaider. Computer generated proofs of binomial multi-sum identities, Master thesis, RISC, J. Kepler University, 1997.

[129] B. Zimmermann, PhD thesis, RISC, Johannes Kepler University Linz, 2007. (In preparation.)

[130] F. Chyzak, *An extension of Zeilberger's fast algorithm to general holonomic functions*, Discrete Math. 217 (2000), 115–134.

[131] F. Chyzak and B. Salvy, *Non-commutative elimination in Ore algebras proves multivariate identities*, J. Symbolic Comput. 26 (1998), 187–227.

[132] G.E. Andrews, R. Askey, R. Roy, Special Functions, Cambride University Press, 1999.

[133] S. Beuchler and J. Schöberl, *Extension operators on tensor product structures in 2d and 3d*, preprint, 2004. (To appear in: Appl. Numer. Math.)

[134] S. Gerhold , M. Kauers, and J. Schöberl, *On a conjectured inequality for a sum of Legendre polynomials*, SFB-Report No. 2006-11, 2006.

References DK Ramlau

[135] Heinz W. Engl, Martin Hanke, and Andreas Neubauer. *Regularization of inverse problems.* Mathematics and its Applications (Dordrecht). 375. Dordrecht: Kluwer Academic Publishers. viii, 321 p., 1996.

[136] Alfred K. Louis. *Inverse und schlecht gestellte Probleme. (Inverse and ill-posed problems).* Teubner Studienbücher: Mathematik. Stuttgart: B. G. Teubner. 205 S., 1989.

[137] David L. Donoho. Nonlinear solution of linear inverse problems by wavelet-vaguelette decomposition. *Appl. Comput. Harmon. Anal.*, 2(2):101–126, 1995.

[138] F. Abramovich and B.W. Silverman. Wavelet decomposition approaches to statistical inverse problems. *Biometrika*, 85(1):115–129, 1998.

[139] A. Cohen, M. Hoffmann, and M. Reiss. Adaptive wavelet Galerkin methods for linear inverse problems. *SIAM J. Numerical Analysis*, 42(4):1479–1501, 2004.

[140] P. Jonas and A.K. Louis. A Sobolev space analysis of linear regularization methods for ill-posed problems. *J. Inverse Ill-posed Probl.*, 9, 2001.

[141] E. Klann, P. Maass and R. Ramlau. *Two-step regularization methods for linear inverse problems. J. Inv. Ill - Posed Prob.*,14(6):583-607,2006.

[142] E. Klann. *Regularization of linear ill-posed problems in two steps: combination of data smoothing and reconstruction methods.* PhD thesis, University of Bremen, 2006.

[143] E. Klann and R. Ramlau. *Regularization by fractional filter methods and data smoothing.* submitted for publication, 2007.

[144] R. Ramlau and G. Teschke. *Regularization of Sobolev Embedding Operators and Applications to Medical Imaging and Meteorological Data. Part I: Regularization of Sobolev Embedding Operators. Sampling Theory in Signal and Image Processing*, Volume 3 (2), 2004.

[145] R. Ramlau and G. Teschke. *Regularization of Sobolev Embedding Operators and Applications to Medical Imaging and Meteorological Data. Part II: Regularization Incorporating Noise with Applications in Medical Imaging and Meteorological Data. Sampling Theory in Signal and Image Processing*, 3(3):2004.

[146] Eric D. Kolaczyk. *Wavelet shrinkage estimates of certain Poisson intensity signals using corrected thresholds. Stat. Sin. 9*, No.1, 119-135, 1999.

[147] Hugh A. Chipman, Eric D. Kolaczyk and Robert E. McCulloch. *Adaptive Bayesian wavelet shrinkage. J.Am.Stat.Assoc. 92*, No.440, 1413-1421, 1997.

[148] X. Huang, A.C. Madoc and A.D. Cheetham. *Wavelet-based Bayesian estimator for Poisson noise removal from images.* Multimedia and Expo, 2003. ICME 2003. Proceedings. 6-9 July 2003 Page(s): I - 593-6 vol.1.

[149] Dirk A. Lorenz. *Non-convex Variational Denoising of Images: Interpolation Between Hard and Soft Wavelet Shrinkage. Current Development in Theory and Applications of Wavelets.* Volume 1, Number 1, p. 31-56 April 2007.

[150] Henning Thielemann. *Optimally matched wavelets.* PhD thesis, University of Bremen, 2006.

[151] Ingrid Daubechies, Michel Defrise, and Christine DeMol. An iterative thresholding algorithm for linear inverse problems with a sparsity constraint. *Commun. Pure Appl. Math.*, 57(11):1413–1457, 2004.

[152] Ronny Ramlau and Gerd Teschke. A Tikhonov-based projection iteration for nonlinear ill-posed problems with sparsity constraints. *Numer. Math.*, vol. 104, no. 2, 2006.

[153] Ingrid Daubechies, Gerd Teschke and Luminita Vese. Iteratively solving linear inverse problems under general convex constraints. *Inverse Problems and Imaging*, 1(1), 2007.

[154] Frank Natterer. Error bounds for Tikhonov regularization in Hilbert scales. *Appl. Anal.*, 18:29–37, 1984.

[155] Peter Mathé and Sergei V. Pereverzev. Optimal discretization of inverse problems in Hilbert scales. Regularization and self-regularization of projection methods. *SIAM J. Numer. Anal.*, 38(6):1999–2021, 2001.

[156] Michael Nussbaum and Sergei Pereverzev. The Degree of Ill-Posedness in Stochastic and Deterministic Models. Technical report, Preprint 509, Weierstraß-Institut, Berlin, 1999.

[157] Bernard A. Mair and Frits H. Ruymgaart. Statistical inverse estimation in Hilbert scales. *SIAM J. Appl. Math.*, 56(5):1424–1444, 1996.

[158] Andreas Neubauer. An a posteriori parameter choice for Tikhonov regularization in Hilbert scales leading to optimal convergence rates. *SIAM J. Numer. Anal.*, 25(6):1313–1326, 1988.

[159] Andreas Neubauer. When do Sobolev spaces form a Hilbert scale ?. *Proc. Am. Math. Soc.*, 103(2):557–562, 1988.

[160] Andreas Neubauer. Tikhonov regularization of nonlinear ill-posed problems in Hilbert scales. *Appl. Anal.*, 46(1-2):59–72, 1992.

[161] Andreas Neubauer. On Landweber iteration for nonlinear ill-posed problems in Hilbert scales. *Numer. Math.*, 85(2):309–328, 2000.

[162] R. Novikov. An inversion formula for the attenuated X-ray transformation. *Ark. Mat.*, Vol. 40, 145-167,2002.

[163] F. Natterer. Inversion of the attenuated Radon transform. *Inverse Problems.* Vol. 17, p. 113-119, 2001.

[164] G. Bal. On the attenuated Radon transform with full and partial measurements. *Inverse Problems.* Vol. 20, 2004.

[165] L. Kunyansky. A new SPECT reconstruction algorithm based on the Novikov explicit inversion formula. *Inverse Problems.*, Vol.17, p.293-306, 2001.

[166] J.-P. Guillement, F. Jauberteau, L. Kunyansky, R. Novikov and R. Trebossen. On single-photon emission computed tomography imaging based on an exact formulafor the nonuniform attenuation correction. *Inverse Problems.* Vol. 18, 2002.

[167] J.-P. Guillement and R. Novikov. A noise property analysis of single-photon emission computed tomography data. *Inverse Problems.* Vol. 20, p. 175-198, 2004.

References DK Schicho

[168] C. Andradas, T. Recio, and R. Sendra. Relatively optimal rational space curve reparametrization through canonical divisors. In *Proc. ISSAC 1997*, pages 349–355. ACM Press, 1997.

[169] T. Beck and J. Schicho. Curve parametrization over optimal field extensions exploiting the Newton polygon. In *Proc. Compass 2005*. Springer, 2007. to appear.

[170] T. Beck and J. Schicho. Parametrization of algebraic curves defined by sparse equations. *AAECC*, 18:127–150, 2007.

[171] A. Campillo, F. Delgado, and S. M. Gusein-Zade. The Alexander polynomial of a plane curve singularity via the ring of functions on it. *Duke Math. J.*, 117(1):125–156, 2003.

[172] G. Chèze and A. Galligo. From an approximate to an exact absolute polynomial factorization. *J. Symbolic Comput.*, 41(6):682–696, 2006.

[173] R. M. Corless, M. Giesbrecht, and D. J. Jeffrey. Approximate polynomial decomposition. In *Proc. ISSAC'99*, pages 213–219. ACM Press, 1999.

[174] R. M. Corless, S. M. Watt, and L. Zhi. QR factoring to compute the GCD of univariate approximate polynomials. *IEEE Trans. Signal Process.*, 52(12):3394–3402, 2004.

[175] D. Eisenbud and W. Neumann. *Three-dimensional link theory and invariants of plane curve singularities*, volume 110 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[176] M. Gahleitner, B. Jüttler, and J. Schicho. Approximate parametrization of planar cubics. In *Curve and Surface Fitting. St. Malo 2002*. Nashboro Press, 2003.

[177] S. Gao, E. Kaltofen, J. P. May, Z. Yang, and L. Zhi. Approximate factorization of multivariate polynomials via differential equations. In *ISSAC 2004*, pages 167–174. ACM, New York, 2004.

[178] J. Gutierrez, R. Rubio, and J. Schicho. Polynomial parametrization of curves without affine singularities. *Comp. Aided Geom. Design*, 19:223–234, 2002.

[179] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symb. Comp.*, 33(4):425–445, 2002.

[180] S. Kusper. Numerical analysis of singularities of plane algebraic curves. Master's thesis, Univ. Linz, 2006.

[181] C. Liang, B. Mourrain, and J. P. Pavone. Subdivision methods for the topology of 2d and 3d implicit curves. In *Proc. Compass 2005*. Springer, 2007. to appear.

[182] M. Mñuk, J. R. Sendra, and F. Winkler. On the complexity of parametrizing curves. *Beitr. Algebra und Geometrie*, 37/2:309–328, 1996.

[183] J. Milnor. *Singular points of complex hypersurfaces*. Annals of Mathematics Studies, No. 61. Princeton University Press, Princeton, N.J., 1968.

[184] S. Pérez-Díaz, J. Sendra, and J. R. Sendra. Parametrization of approximate algebraic curves by lines. *Theoret. Comp. Sci.*, 315:627–650, 2004.

[185] J. Schicho. Simplification of surface parametrizations – a lattice polygon approach. *J. Symb. Comp.*, 36:535–554, 2003.

[186] J.R. Sendra and F. Winkler. Symbolic parametrization of curves. *J. Symb. Comp.*, 12(6):607–632, 1991.

[187] J.R. Sendra and F. Winkler. Parametrization of algebraic curves over optimal field extensions. *J. Symb. Comp.*, 23(2/3):191–208, 1997.

[188] H.-J. Stetter. *Numerical polynomial algebra*. SIAM, Philadelphia, 2004.

[189] S. Fiedler-Le Touzé. Pencils of cubics as tools to solve an interpolation problem. *Appl. Algebra Engrg. Comm. Comput.*, 18(1-2):53–70, 2007.

[190] C. L. Bajaj A. V. and Royappa. Parameterization in finite precision. *Algorithmica*, 27(1):100–114, 2000. Implementation of geometric algorithms.

[191] M. van Hoeij. Rational parametrizations of algebraic curves using canonical divisors. *J. Symb. Comp.*, 23:209–227, 1997.

[192] Z. Zeng and B. H. Dayton. The approximate GCD of inexact polynomials. II. A multivariate algorithm. In *ISSAC 2004*, pages 320–327. ACM, New York, 2004.

References DK Schreiner

[193] J.-R. Abrial. *The B-Book: Assigning Programs to Meanings*. Cambridge University Press, Cambridge, UK, 1996.

[194] A. A. Adams, H. Gottliebsen, S. A. Linton, and U. Martin. Automated Theorem Proving in Support of Computer Algebra: Symbolic Definite Integration as a Case Study. In *ISSAC '99: International Symposium on Symbolic and Algebraic Computation*, pages 253–260, Vancouver, British Columbia, Canada, 1999. ACM Press, New York.

[195] A. A. Adams, Hanne Gottliebsen, Steve Linton, and Ursula Martin. VSDITLU: A Verifiable Symbolic Definite Integral Table Look-Up. In Harald Ganzinger, editor, *CADE-16, 16th International Conference on Automated Deduction*, volume 1632 of *Lecture Notes in Computer Science*, pages 112–126, Trento, Italy, July 7–10, 1999. Springer.

[196] Andrew Adams, Martin Dunstan, Hanne Gottliebsen, Tom Kelsey, Ursula Martin, and Sam Owre. Computer Algebra Meets Automated Theorem Proving: Integrating Maple and PVS. In Richard J. Boulton and Paul B. Jackson, editors, *TPHOLs 2001: 14th International Conference on Theorem Proving in Higher Order Logics*, volume 2152 of *Lecture Notes in Computer Science*, pages 27–42, Edinburgh, Scotland, UK, September 3–6, 2001. Springer.

[197] Aldor, 2007. http://www.aldor.org.

[198] Alessandro Armando and Daniele Zini. Towards Interoperable Mechanized Reasoning Systems: the Logic Broker Architecture. In Antonio Corradi, Andrea Omicini, and Agostino Poggi, editors, *WOA 2000: 1st AI*IA/TABOO Joint Workshop "From Objects to Agents": Evolutive Trends of Software Systems*, pages 70–75, Parma, Italy, May 29–30, 2000. Pitagora Editrice Bologna.

[199] Clemens Ballarin, Karsten Homann, and Jacques Calmet. Theorems and Algorithms: an Interface between Isabelle and Maple. In *ISSAC '95: International Symposium on Symbolic and Algebraic Computation*, pages 150–157, Montreal, Quebec, Canada, July 10–12, 1995. ACM Press, New York.

[200] Clemens Ballarin and Lawrence C. Paulson. A Pragmatic Approach to Extending Provers by Computer Algebra - with Applications to Coding Theory. *Fundamenta Informaticae*, 39(1–2):1–20, 1999.

[201] Rebhi Baraka. *A Framework for Publishing and Discovering Mathematical Web Services*. PhD thesis, Johannes Kepler University, Linz, Austria, August 2006.

[202] Rebhi Baraka, Olga Caprotti, and Wolfgang Schreiner. A Web Registry for Publishing and Discovering Mathematical Services. In Wiliam Cheung and Jane Hsu, editors, *IEEE EEE'05: IEEE Conference on e-Technology, e-Commerce, and e-Service*, pages 190–193. IEEE Computer Society, March 21 – April 1 2005.

[203] Rebhi Baraka and Wolfgang Schreiner. Querying Registry-Published Mathematical Web Services. In *AINA'2006: IEEE 20th International Conference on Advanced Informati on Networking and Applications*, pages 767–772, Vienna, Austria, April 18–20, 2006. IEEE Computer Society Press.

[204] Rebhi Baraka and Wolfgang Schreiner. Semantic Querying of Mathematical Web Service Descriptions. In M. Bravetti, M. Nunez, , and Gianluigi Zavattaro, editors, *WS-FM 2006: Third International Workshop on Web Services and Formal Methods, Vienna, Austria, September 8–9*, volume 4184 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2006.

[205] Mike Barnett, K. Rustan M. Leino, and Wolfram Schulte. The Spec# Programming System: An Overview. In *CASSIS'2004: International Workshop on Construction and Analysis of Safe, Secure, and Interoperable Smart Devices*, volume 3362 of *Lecture Notes in Computer Science*, pages 49–69, Marseille, France, March 10–13, 2004. Springer, Berlin.

[206] Clark Barrett and Sergey Berezin. CVC Lite: A New Implementation of the Cooperating Validity Checker. In *Computer Aided Verification: 16th International Conference, CAV 200 4, Boston, MA, USA, July 13–17, 2004*, volume 3114 of *LNCS*, pages 515–518. Springer, 2004.

[207] David A. Basin, Yves Deville, Pierre Flener, Andreas Hamfelt, and Jørgen Fischer Nilsson. Synthesis of Programs in Computational Logic. In Maurice Bruynooghe and Kung-Kiu Lau, editors, *Program Development in Computational Logic: A Decade of Research Advances in Logic-Based Program Development*, volume 3049 of *Lecture Notes in Computer Science*, pages 30–65. Springer, 2004.

[208] Andrej Bauer, Edmund Clarke, and Xudong Zhao. Analytica — An Experiment in Combining Theorem Proving and Symbolic Computation. *Journal of Automated Reasoning*, 21(3):295–325, 1998.

[209] Bernhard Bauer and Rolf Hennicker. Proving the Correctness of Algebraic Implementations by the ISAR System. In Alfonso Miola, editor, *DISCO '93: Design and Implementation of Symbolic Computation Systems, International Symposium*, volume 722 of *Lecture Notes in Computer Science*, pages 2–16, Gmunden, Austria, September 15–17, 1993. Springer.

[210] Bernhard Beckert, Reiner Hähnle, and Peter H. Schmitt, editors. *Verification of Object-Oriented Software: The KeY Approach*. Springer, 2007.

[211] Piergiorgio Bertoli, Jacques Calmet, Fausto Giunchiglia, and Karsten Homann. Specification and Integration of Theorem Provers and Computer Algebra Systems. *Fundam. Inform.*, 39(1-2):39–57, 1999.

[212] Wieb Bosma, John Cannon, and Graham Matthews. Programming with Algebraic Structures: Design of the MAGMA Language. In *ISSAC '94: International Symposium on Symbolic and Algebraic Computation*, pages 52–57, Oxford, UK, July 20–22, 1994. ACM Press, NY.

[213] Sylvain Boulmé, Thérèse Hardin, Daniel Hirschkoff, Valérie Ménissier-Morain, and Renaud Rioboo. On the Way to Certify Computer Algebra Systems. *Electronic Notes in Theoretical Computer Science*, 23(3), 1999.

[214] Bruno Buchberger and Adrian Craciun. Algorithm Synthesis by Lazy Thinking: Using Problem Schemes. In D.Petcu, V. Negru, D. Zaharie, and T. Jebelean, editors, *SYNASC 2004: 6th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 90–106, Timisoara, Romania, September 26–30, 2004. Mirton.

[215] Bruno Buchberger, Adrian Craciun, Tudor Jebelean, et al. Theorema: Towards Computer-Aided Mathematical Theory Exploration. *Journal of Applied Logic*, 4(4):470–504, 2006.

[216] Bruno Buchberger, Tudor Jebelean, et al. A Survey of the Theorema Project. In Wolfgang Küchlin, editor, *ISSAC'97 International Symposium on Symbolic and Algebraic Computat ion*, pages 384–391, Maui, Hawaii, July 21–23, 1997. ACM Press, New York.

[217] Lilian Burdy, Yoonsik Cheon, David Cok, Michael D. Ernst, Joe Kiniry, Gary T. Leavens, K. Rustan M. Leino, and Erik Poll. An Overview of JML Tools and Applications. *Software Tools for Technology Transfer*, 7(3):212–232, June 2005.

[218] Jacques Calmet and Karsten Homann. Classification of Communication and Cooperation Mechanisms for Logical and Symbolic Computation Systems. In F. Baader and K. U. Schulz, editors, *FroCos 1996: 1st International Workshop on Frontiers of Combining Systems*, pages 221–234, Munich, Germany, 1996. Kluwer Academic Publishers.

[219] Jacques Calmet and Indra A. Tjandra. A Unified-Algebra-Based Specification Language for Symbolic Computing. In Alfonso Miola, editor, *DISCO'93: Design and Implementation of Symbolic Computation Systems*, volume 722 of *Lecture Notes in Computer Science*, pages 122–133, Gmunden, Austria, September 15–17, 1993. Springer.

[220] Olga Caprotti and Wolfgang Schreiner. Towards A Mathematical Services Description Language. In Arjeh M. Cohen, Xiao-Shan Gao, and Nobuki Takayama, editors, *ICMS'2002: International Congress of Mathematical Software, Beijing, China. August 17 – 19*. World Scientific Publishers, Singapore/River Edge, 2002.

[221] Olga Caprotti and Volker Sorge. Integration of Automated Reasoning and Computer Algebra Systems. *Journal of Symbolic Computation*, 39(5):501–502, 2005.

[222] Gareth Carter, Rosemary Monahan, and Joseph M. Morris. Software Refinement with Perfect Developer. In *SEFM'05: Third IEEE International Conference on Software Engineerin g and Formal Methods*, pages 363–373, Koblenz, Germany, September 5–9, 2005. IEEE Computer Society.

[223] Kalisyk Cezary and Freek Wiedijk. Certified Computer Algebra on Top of an Interactive Theorem Prover. In *Calculemus 2007 — 14th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning*, LNAI, Hagenberg, Austria, June 27–30, 2007. Springer.

[224] Patrice Chalin, Joseph R. Kiniry, Gary T. Leavens, and Erik Poll. Beyond Assertions: Advanced Specification and Verification with JML and ESC/Java2. In *Formal Methods for Components and Objects (FMCO) 2005, Revised Lectures*, volume 4111 of *Lecture Notes in Computer Science*, pages 342–363. Springer, 2006.

[225] Gianna Cioni, Attilio Colagrossi, and Marco Temperini. An Approach to Class Reasoning in Symbolic Computation. In Jacques Calmet and Carla Limongelli, editors, *DISCO'96: Design and Implementation of Symbolic Computation Systems*, volume 1128 of *Lecture Notes in Computer Science*, pages 240–251, Karlsruhe, Germany, September 18-20, 1996. Springer.

[226] E. M. Clarke, A. S. Gavlovski, K. Sutner, and W. Windsteiger. Analytica V: Towards the Mordell-Weil Theorem. In A. Bigatti and S. Ranise, editors, *Calculemus'06, 13th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning*, Genova, Italy, July 2–6, 2006.

[227] H. Comon, M. Dauchet, R. Gilleron, F. Jacquemard, D. Lugiez, S. Tison, and M. Tommasi. Tree Automata Techniques and Applications. http://www.grappa.univ-lille3.fr/tata, September 2005.

[228] Robert M. Corless and David J. Jeffrey. Well ... it isn't quite that simple. *SIGSAM Bulletin*, 26(3):2–6, 1992.

[229] James H. Davenport. Abstract Data Types in Computer Algebra. In Mogens Nielsen and Branislav Rovan, editors, *MFCS 2000: International Symposium on Mathematical Foundations of Computer Science 2000*, volume 1893 of *Lecture Notes in Computer Science*, pages 21–35, Bratislava, Slovakia, August 28 – September 1, 2000. Springer.

[230] James H. Davenport. Equality in Computer Algebra and Beyond. *Journal of Symbolic Computation*, 34(4):259–270, 2002.

[231] Andreas Dolzmann and Thomas Sturn. REDLOG: Computer Algebra Meets Computer Logic. *SIGSAM Bulletin*, 31(2):2–9, 1997.

[232] César Domínguez, Laureano Lambán, Vico Pascual, and Julio Rubio. Hidden Specification of a Functional System. In Roberto Moreno-Díaz, Bruno Buchberger, and José Luis Freire, editors, *Computer Aided Systems Theory - EUROCAST 2001*, volume 2178 of *Lecture Notes in Computer Science*, pages 555–569, Las Palmas, de Gran Canaria, Spain, February 19–23, 2001. Springer.

[233] César Domínguez and Julio Rubio. Modeling Inheritance as Coercion in a Symbolic Computation System. In *ISSAC '01: International Symposium on Symbolic and Algebraic Computation*, pages 109–115. ACM Press, New York, 2001.

[234] Martin Dunstan, Tom Kelsey, Steve Linton, and Ursula Martin. Lightweight Formal Methods for Computer Algebra Systems. In Oliver Gloor, editor, *ISSAC 1998: International Symposium on Symbolic and Algebraic Computation*, pages 80–87, Rostock, Germany, August 13–15, 1998. ACM Press.

[235] Martin Dunstan, Tom Kelsey, Ursula Martin, and Steve Linton. Formal Methods for Extensions to CAS. In Jeannette M. Wing, Jim Woodcock, and Jim Davies, editors, *FM'99 - World Congress on Formal Methods in the Development of Computing Systems*, volume 1709 of *Lecture Notes in Computer Science*, pages 1758–1777, Toulouse, France, September 20-24, 1999. Springer.

[236] David Evans, John Guttag, James Horning, and Yang Meng Tan. LCLint: A Tool for Using Specifications to Check Code. In *ACM SIGSOFT '94 Symposium on the Foundations of Software Engineering*, pages 87–96, 1994.

[237] Richard J. Fateman. Why Computer Algebra Systems Sometimes Can't Solve Simple Equations. *SIGSAM Bulletin*, 30(2):8–11, 1996.

[238] Stéphane Fechter. An Object-Oriented Model for the Certified Computer Algebra Library. In *FMOODS 2002, Formal Methods for Open Object-Based Distributed Systems, PhD workshop*, Twente, The Netherlands, March 20–22, 2002.

[239] Hanne Gottliebsen, Tom Kelsey, and Ursula Martin. Hidden Verification for Computational Mathematics. *Journal of Symbolic Computation*, 39(5):539–567, 2005.

[240] Benjamin Grégoire and Assia Mahboubi. Proving Equalities in a Commutative Ring Done Right in Coq. In Joe Hurd and Thomas F. Melham, editors, *TPHOls 2005, Theorem Proving in Higher Order Logics, 18th International Conference*, volume 3603 of *Lecture Notes in Computer Science*, Oxford, UK, August 22–25, 2005. Springer.

[241] John Harrison and L. Théry. A Skeptic's Approach to Combining HOL and Maple. *Journal of Automated Reasoning*, 21(3):279–294, 1998.

[242] John Harrison and Laurent Théry. Extending the HOL Theorem Prover with a Computer Algebra System to Reason about the Reals. In Jeffrey J. Joyce and Carl Seger, editors, *1993 International Workshop on the HOL Theorem Proving System and its Applications*, volume 780 of *Lecture Notes in Computer Science*, pages 174–184, Vancouver, Canada, August 1993. Springer.

[243] John Harrison and Laurent Théry. Reasoning About the Reals: the Marriage of HOL and Maple. In Andrei Voronkov, editor, *LPAR '93: 4th International Conference on Logic Programming and Automated Reasoning*, volume 698 of *Lecture Notes in Computer Science*, St. Petersburg, Russia, July 13–20, 1993. Springer.

[244] C. A. R. Hoare. Proof of Correctness of Data Representations. *Acta Informatica*, 1:271–281, 1972.

[245] Pietro Iglio and Giuseppe Attardi. Software Components for Computer Algebra. In *ISSAC '98: 1998 International Symposium on Symbolic and Algebraic Computation*, pages 62–69, Rostock, Germany, August 13–15, 1998. ACM Press, New York.

[246] Andrew Ireland, Bill J. Ellis, et al. An Integrated Approach to High Integrity Software Verification. *Journal of Automated Reasoning*, 36(4):379–410, 2006.

[247] Daniel Jackson. *Software Abstractions — Logic, Language, and Analysis*. MIT Press, Cambridge, MA, 2006.

[248] Cliff B. Jones. *Systematic Software Development Using VDM*. Prentice-Hall, Upper Saddle River, NJ, 1990.

[249] Richard Jüllig, Yellamraju V. Srinivas, and J. Liu. SPECWARE: An Advanced Evironment for the Formal Development of Complex Software Systems. In Martin Wirsing and Maurice Nivat, editors, *AMAST '96: 5th International Conference on Algebraic Methodology and Software Technology*, volume 1101 of *Lecture Notes in Computer Science*, pages 551–554, Munich, Germany, July 1–5, 1996, 1996. Springer.

[250] Tom Kelsey. *Formal Methods and Computer Algebra: A Larch Specification of AXIOM Categories and Functors*. PhD thesis, School of Mathematical and Computational Sciences, University of St Andrews, December 1999.

[251] Robert Klapper and Aaron Stump. Validated Proof-Producing Decision Procedures. *Electronic Notes in Theoretical Computer Science*, 125(3):53–68, July 2005.

[252] Anneke Kleppe and Jos Warmer. An Introduction to the Object Constraint Language (OCL). In *TOOLS 2000: 33rd International Conference on Technology of Object-Oriented Languages and Systems*, page 456, St. Malo, France, June 5–8, 2000. IEEE Computer Society.

[253] Laureano Lambán, Vico Pascual, and Julio Rubio. Specifying Implementations. In *ISSAC '99: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, pages 245–251, Vancouver, British Columbia, Canada, July 29–31, 1999. ACM Press, New York.

[254] Laureano Lambán, Vico Pascual, and Julio Rubio. An Object-oriented Interpretation of the EAT System. *Appl. Algebra Eng. Commun. Comput.*, 14(3):187–215, 2003.

[255] Gary T. Leavens, Albert L. Baker, and Clyde Ruby. JML: A Notation for Detailed Design. In Haim Kilov, Bernhard Rumpe, and Ian Simmonds, editors, *Behavioral Specifications of Businesses and Systems*, pages 175–188. Kluwer Academic Publishers, 1999.

[256] Gary T. Leavens and Yoonsik Cheon. Preliminary Design of Larch/C++. In U. Martin and J. Wing, editors, *First First International Workshop on Larch*, Workshops in Computing Science, pages 159–184, Deadham, MA, July 13–15, 1992. Springer, Berlin.

[257] Carla Limongelli and Marco Temperini. Abstract Specification of Structures and Methods in Symbolic Mathematical Computation. *Theoretical Computer Science*, 104(1):89–107, 1992.

[258] Assia Mahboubi. Programming and Certifying a CAD Algorithm in the Coq System. In Thierry Coquand, Henri Lombardi, and Marie-Françoise Roy, editors, *Mathematics, Algorithms, Proofs*, number 05021 in Dagstuhl Seminar Proceedings. IBFI, Germany, 2005.

[259] Assia Mahboubi. Proving Formally the Implementation of an Efficient gcd Algorithm for Polynomials. In Ulrich Furbach and Natarajan Shankar, editors, *IJCAR 2006, Third International Joint Conference on Automated Reasoning*, volume 4130 of *Lecture Notes in Computer Science*, pages 438–452, Seattle, WA, USA, August 17–20, 2006. Springer.

[260] Assia Mahboubi. Implementing the Cylindrical Algebraic Decomposition within the Coq System. *Mathematical Structures in Computer Science*, 17(1):99–127, 2007.

[261] Ursula Martin. Computers, Reasoning and Mathematical Practice. In *Computational Logic, 1997 NATO ASI Summer School on Logic and Computation*, volume 165 of *NATO Advanced Science Institute Series For Computational Systems Sciences*, pages 301–346. Springer, Berlin, Marktoberdorf, Germany, 1997.

[262] MathBroker II - Brokering Distributed Mathematical Services, 2007. http://www.risc.uni-linz.ac.at/projects/mathbroker2.

[263] Sean McLaughlin and John Harrison. A Proof-Producing Decision Procedure for Real Arithmetic. In Robert Nieuwenhuis, editor, *CADE-20: 20th International Conference on Automated Deduction*, volume 3632 of *Lecture Notes in Computer Science*, pages 295–314, Tallinn, Estonia, July 22–27, 2005. Springer.

[264] Henrik Persson. Certified Computer Algebra. In *Types summer school'99: Theory and practice of formal proofs*, Giens, France, August 30 – September 10, 1999. INRIA.

[265] Erik Poll and Simon Thompson. Adding the Axioms to Axiom: Towards a System of Automated Reasoning in Aldor. In *Calculemus and Types '98*, Eindhoven, The Netherlands, July 13–15, 1998.

[266] Erik Poll and Simon Thompson. Integrating Computer Algebra and Reasoning through the Type System of Aldor. In Helene Kirchner and Christophe Ringeissen, editors, *Frocos 2000, Frontiers of Combining Systems*, volume 1794 of *Lecture Notes in Computer Science*, pages 136–150, Nancy, France, March 22–24, March 2000. Springer.

[267] Virgile Prevosto. Certified Mathematical Hierarchies: the FoCal System. In Thierry Coquand, Henri Lombardi, and Marie-Françoise Roy, editors, *Mathematics, Algorithms, Proofs*, volume 05021 of *Dagstuhl Seminar Proceedings*, Schloss Dagstuhl, Germany, January 9–14, 2005. IBFI, Schloss Dagstuhl, Germany.

[268] The RISC ProofNavigator, 2006. Research Institute for Symbolic Computation (RISC), Johannes Kepler Univ ersity, Linz, Austria, http://www.risc.uni-linz.ac.at/research/formal/software /ProofNavigator.

[269] John Rushby. Disappearing Formal Methods. In *HASE'00: Fifth IEEE International Symposium on High-Assurance Systems Engineering Symposium*, pages 95–96, Albuquerque, NM, November 2000. ACM, New York.

[270] Philip S. Santas. A Type System for Computer Algebra. *Journal of Symbolic Compututation*, 19(1–3):79–109, 1995.

[271] Wolfgang Schreiner. Program Verification with the RISC ProofNavigator. In *Teaching Formal Methods: Practice and Experience*, Electronic Workshops in Computing (eWiC), BCS-FACS Christmas Meeting, London, UK, December 15, 2006. British Computer Society.

[272] SMT-LIB — The Satisfiability Modulo Theories Library, 2006. University of Iowa, Iowa City, IA,
http://combination.cs.uiowa.edu/smtlib.

[273] Volker Sorge. Non-Trivial Symbolic Computations in Proof Planning. In Hélène Kirchner and Christophe Ringeissen, editors, *FroCoS 2000: Third International Workshop on Frontiers of Combining Systems*, volume 1794 of *Lecture Notes in Computer Science*, pages 121–135, Nancy, France, March 22-24, 2000, 2000. Springer.

[274] David R. Stoutemyer. Crimes and Misdemeanors in the Computer Algebra Trade. *Notices of the American Mathematical Society*, 38(7):778–785, September 1991.

[275] Carolyn L. Talcott. A Theory for Program and Data Type Specification. *Theoretical Compututer Science*, 104(1):129–159, 1992.

[276] Overview of Theorema, 2006. Research Institute for Symbolic Computation (RISC), Johannes Kepler Unive rsity, Linz, Austria, http://www.risc.uni-linz.ac.at/research/theorema.

[277] Laurent Théry. A Certified Version of Buchberger's Algorithm. In *CADE-15: 15th International Conference on Automated Deduction*, number 1421 in LNAI, pages 349–364, Lindau, Germany, July 5–10, 1998. Springer-Verlag.

[278] Simon Thompson. Logic and Dependent Types in the Aldor Computer Algebra System. In Manfred Kerber and Michael Kohlhase, editors, *Calculemus 2000: Symbolic Computation and Automated Reasoning*, pages 205–219, St. Andrews, Scotland, August 6–7, 2000. A. K. Peters, Natick, MA.

[279] Simon Thompson, John Shackell, James Beaumont, and Leonid Timochouk. Atypical: Integrating Computer Algebra and Reasoning, 2003. http://www.cs.kent.ac.uk/people/staff/sjt/Atypical.

[280] Michael J. Wester. A Critique of the Mathematical Abilities of CA Systems. In Michael J. Wester, editor, *Contents of Computer Algebra Systems: A Practical Guide*. John Wiley & Sons, Chichester, UK, 1999.

[281] Jim Woodcock and Jim Davies. *Using Z: Specification, Refinement, and Proof*. Prentice-Hall, Inc., Upper Saddle River, NJ, 1996.

References DK Winkler

[282] R. Gebauer, M. Kalkbrener, B. Wall, F. Winkler, *CASA: A Computer Algbra Package for Constructive Algebraic Geometry*, in Proc. ISSAC'1991, S.M.Watt (ed.), ACM-Press, 403–410

[283] J.R. Sendra, F. Winkler, *Symbolic Parametrization of Curves*, J. of Symbolic Computation 12/6 (1991), 607–631

[284] F. Winkler, *Parametrized Solutions of Algebraic Equations*, J. Mathematics and Computers in Simulation 42/4-6 (1996), 333–338

[285] F. Winkler, *Algebraic Computation in Geometry*, J. Mathematics and Computers in Simulation 42/4-6 (1996), 529–537

[286] M. Mňuk, J.R. Sendra, F. Winkler, *On the Complexity of Parametrizing Curves*, Beiträge zur Algebra und Geometrie 37/2 (1996), 309–328

[287] M. Mňuk, F. Winkler, *CASA — A System for Computer Aided Constructive Algebraic Geometry*, in Lecture Notes in Computer Science 1128, J.Calmet and C.Limongelli (eds.), Springer-Verlag, 297–307 (1996)

[288] J.R. Sendra, F. Winkler, *Parametrization of Algebraic Curves over Optimal Field Extensions*, J. Symbolic Computation 23/2&3 (1997), 191–207

[289] E. Hillgarter, F. Winkler, *Points on Algebraic Curves and the Parametrization Problem*, in Lecture Notes in Computer Science 1360, D.Wang (ed.), Springer-Verlag, 189–207 (1998)

[290] J.R. Sendra, F. Winkler, *Algorithms for Rational Real Algebraic Curves*, Fundamenta Informaticae 39/1-2 (1999), 211–228

[291] G. Landsmann, J. Schicho, F. Winkler, E. Hillgarter, *Symbolic Parametrization of Pipe and Canal Surfaces*, in Proc. ISSAC'2000, C.Traverso (ed.), 202–208, ACM-Press, 2000

[292] G. Landsmann, J. Schicho, F. Winkler, *The Parametrization of Canal Surfaces and the Decomposition of Polynomials into a Sum of Two Squares*, J. Symbolic Computation 32/1&2 (2001), 119–132

[293] J.R. Sendra, F. Winkler, *Computation of the Degree of a Rational Map between Curves*, in Proc. ISSAC'2001, B.Mourrain (ed.), 317–322, ACM-Press, 2001

[294] J.R. Sendra, F. Winkler, *Tracing Index of Rational Curve Parametrizations*, Computer Aided Geometric Design 18 (2001), 771–795

[295] R. Hemmecke, E. Hillgarter, F. Winkler, *CASA*, in Handbook of Computer Algebra: Foundations, Applications, Systems, J.Grabmeier, E.Kaltofen, V.Weispfenning (eds.), 356–359, Springer-Verlag, 2003

[296] J.R. Sendra, F. Winkler, S. Pérez-Díaz, *Rational Algebraic Curves — A Computer Algebra Approach*, book to be published by Springer-Verlag Heidelberg, in series "Computational Mathematics"

[297] D. Poulakis, E. Voskos, *On the Practical Solutions of Genus Zero Diophantine Equations*, J. Symbolic Computation 30 (2000), 573–582

[298] D. Poulakis, E. Voskos, *Solving Genus Zero Diophantine Equations with at Most Two Infinity Valuations*, J. Symbolic Computation 33 (2002), 479–491

[299] R. Feng, X.-S. Gao, *Rational General Solutions of Algebraic Ordinary Differential Equations*, in Proc. ISSAC'2004, J.Gutierrez (ed.), 155–162, ACM-Press, 2004

References DK Zulehner

[300] G. Al-Jeiroudi, J. Gondzio, and J. Hall. Preconditioning indefinite systems in interior point methods for large scale linear optimization. Technical Report MS-2006-003, School of Mathematics, The University of Edinburgh, 2006.

[301] Eyal Arian and Shlomo Ta'asan. Multigri one-shot methods for optimal control problems: Infinite dimensional control. ICASE-Report 94-52, NASA Langley Research Center, Hampton VA, 1994.

[302] K. Arrow, L. Hurwicz, and H. Uzawa. *Studies in Nonlinear Programming*. Stanford University Press, Stanford, CA, 1958.

[303] R. E. Bank, B. D. Welfert, and H. Yserentant. A class of iterative methods for solving saddle point problems. *Numer. Math.*, 56:645 – 666, 1990.

[304] A. Battermann and M. Heinkenschloss. Preconditioners for Karush-Kuhn-Tucker matrices arising in the optimal control of distributed systems. In *Desch, W. (ed.) et al., Control and Estimation of Distributed Parameter Systems. Int. Ser. Numer. Math. 126*, pages 15–32. Basel: Birkhäuser., 1998.

[305] Astrid Battermann and Ekkehard W. Sachs. Block preconditioners for KKT systems in PDE-governed optimal control problems. In *Hoffmann, Karl-Heinz (ed.) et al., Fast solution of discretized optimization problems. Int. Ser. Numer. Math. 138*, pages 1–18. Basel: Birkhäuser., 2001.

[306] M. Benzi, G. H. Golub, and J. Liesen. Numerical Solution of Saddle Point Problems. *Acta Numerica*, 14:1–137, 2005.

[307] M. Benzi and V. Simoncini. On the eigenvalues of a class of saddle point matrices. *Numer. Math.*, 103(2):173–196, 2006.

[308] George Biros and Omar Ghattas. Parallel Lagrange-Newton-Krylov-Schur methods for PDE-constrained optimization. Part I: The Krylov-Schur solver. *SIAM J. Sci. Comput.*, 27(2):687–713, 2005.

[309] George Biros and Omar Ghattas. Parallel Lagrange-Newton-Krylov-Schur methods for PDE-constrained optimization. Part II: The Lagrange-Newton solver and its application to optimal control of steady viscous flows. *SIAM J. Sci. Comput.*, 27(2):714–739, 2005.

[310] Alfio Borzi, Karl Kunisch, and Do Y. Kwak. Accuracy and convergence properties of the finite difference multigrid solution of an optimal control optimality system. *SIAM J. Control Optimization*, 41(5):1477–1497, 2003.

[311] D. Braess and R. Sarazin. An efficient smoother for the Stokes problem. *Appl. Numer. Math.*, 23(1):3–19, 1997.

[312] J. H. Bramble and J. E. Pasciak. A preconditioning technique for indefinite systems resulting from mixed approximations of elliptic problems. *Math. Comp.*, 50:1 – 17, 1988.

[313] J. H. Bramble, J. E. Pasciak, and A. T. Vassilev. Analysis of the inexact Uzawa algorithm for saddle point problems. *SIAM J. Numer. Anal.*, 34:1072 – 1092, 1997.

[314] Achi Brandt and Nathan Dinar. Multigrid solutions to elliptic flow problems. Numerical methods for partial differential equations, Proc. adv. Semin., Madison 1978, 53-147 (1979)., 1979.

[315] H. S. Dollar. *Iterative Linear Algebra for Constrained Optimization*. PhD thesis, University of Oxford, 2005.

[316] H. S. Dollar, N. I. M. Gould, W. H. A. Schilders, and A. J. Wathen. Implicit-factorization preconditioning and iterative solvers for regularized saddle-point systems. *SIAM J. Matrix Anal. Appl.*, 28(1):170–189, 2006.

[317] Thomas Dreyer, Bernd Maar, and Volker Schulz. Multigrid optimization in applications. *J. Comput. Appl. Math.*, 120(1-2):67–84, 2000.

[318] N. Dyn and W. E. Ferguson. The numerical solution of equality-constrained quadratic programming problems. *Math. Comput.*, 41:165–170, 1983.

[319] H. C. Elman and G. H. Golub. Inexact and preconditioned Uzawa algorithms for saddle point problems. *SIAM J. Numer. Anal.*, 31:1645 – 1661, 1994.

[320] B. Fischer, A. Ramage, D.J. Silvester, and A.J. Wathen. Minimum residual methods for augmented systems. *BIT*, 38(3):527–543, 1998.

[321] M. Fortin and R. Glowinski. *Augmented Lagrangian Methods: Application to the Numerical Solution of Boundary–Value Problems*. North–Holland, Amsterdam, 1983.

[322] Gabriel N. Gatica and Norbert Heuer. A dual-dual formulation for the coupling of mixed FEM and BEM in hyperelasticity. *SIAM J. Numer. Anal.*, 38(2):380–400, 2000.

[323] Gabriel N. Gatica and Norbert Heuer. Conjugate gradient method for dual-dual mixed formulations. *Math. Comput.*, 71(240):1455–1472, 2002.

[324] G. H. Golub and C. Greif. On solving block-structured indefinite linear systems. *SIAM J. Sci. Comput.*, 24(6):2076–2092, 2003.

[325] G. H. Golub, C. Greif, and J. M. Varah. An algebraic analysis of a block diagonal preconditioner for saddle point problems. *SIAM J. Matrix Anal. Appl.*, 27(3):779–792, 2006.

[326] N. I. M. Gould, M. E. Hribar, and J. Nocedal. On the solution of equality constrained quadratic programming arising in optimization. *SIAM J. Sci. Comput.*, 23(4):1376–1395, 2001.

[327] W. Hackbusch. Fast solution of elliptic control problems. *J. Optimization Theory Appl.*, 31:565–581, 1980.

[328] Subhendu Bikash Hazra and Volker Schulz. Simultaneous pseudo-timestepping for PDE-model based optimization problems. *BIT*, 44(3):457–472, 2004.

[329] C. Keller, N. I. M. Gould, and A. J. Wathen. Constraint preconditioning for indefinite linear systems. *SIAM J. Matrix Anal. Appl.*, 21(4):1300–1317, 2000.

[330] Ulrich Langer, Günther Of, Olaf Steinbach, and Walter Zulehner. Inexact Data-Sparse Boundary Element Tearing and Interconnecting Methods. RICAM-Report 2005-07, Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, 2005. (Accepted for publication in SIAM J.Sci.Comput.).

[331] Ulrich Langer, Günther Of, Olaf Steinbach, and Walter Zulehner. Inexact Fast Multipole Boundary Element Tearing and Interconnecting Methods. In Olof Widlund and David Keyes, editors, *Domain Decomposition in Science and Engineering XVI*, volume 55 of *Lecture Notes in Computational Science and Engineering*, pages 404 – 414, New York, 2007. Springer-Verlag.

[332] M. Rozložník and V. Simoncini. Krylov subspace methods for saddle point problems with indefinite preconditioning. *SIAM J. Matrix Anal. Appl.*, 24(2):368–391, 2002.

[333] T. Rusten and R. Winther. A preconditioned iterative method for saddle-point problems. *SIAM J. Matrix Anal. Appl.*, 13:887 – 904, 1992.

[334] J. Schöberl and W. Zulehner. On Schwarz-type smoothers for saddle point problems. *Numer. Math.*, 95:377 – 399, 2003.

[335] J. Schöberl and W. Zulehner. Symmetric Indefinite Preconditioners for Saddle Point Problems with Applications to PDE-Constrained Optimization Problems. SFB-Report 2006-19, SFB F013, Johannes Kepler University Linz, Austria, 2006. (Accepted for publication in SIAM J. Matrix Anal. Appl.).

[336] D. Silvester and A. Wathen. Fast iterative solutions of stabilized Stokes systems. Part II: Using block diagonal preconditioners. *SIAM J. Numer. Anal.*, 31:1352 – 1367, 1994.

[337] R. Simon and W. Zulehner. On Schwarz-type Smoothers for Saddle Point Problems with Applications to PDE-constrained Optimization Problems. SFB-Report 2007-01, SFB F013, Johannes Kepler University Linz, Austria, 2007.

[338] R. Stainko. *Advanced Multilevel Techniques to Topology Optimization*. PhD thesis, Johannes Kepler University Linz, 2006.

[339] R. Stainko and M. Burger. A one-shot approach to topology optimization with stress constraints. In M. P. Bendsoe, N. Olhoff, and O. Sigmund, editors, *IUTAM Symposium on Topological Design Optimization of Structures, Machines, and Materials*, pages 181 – 184. Springer, 2006.

[340] Shlomo Ta'asan. "One-shot" methods for optimal control of distributed parameter systems I: The finite dimensional case. ICASE-Report 91-2, NASA Langley Research Center, Hampton VA, 1991.

[341] S.P. Vanka. Block-implicit multigrid calculation of two-dimensional recirculating flows. *Comput. Methods Appl. Mech. Eng.*, 59:29–48, 1986.

[342] P. Vassilevski and R. Lazarov. Preconditioning mixed finite element saddle-point elliptic problems. *Numer. Linear Algebra Appl.*, 3:1 – 20, 1996.

[343] Markus Wabro. Coupled algebraic multigrid methods for the Oseen problem. *Comput. Vis. Sci.*, 7(3-4):141–151, 2004.

[344] Markus Wabro. AMGe—coarsening strategies and application to the Oseen equations. *SIAM J. Sci. Comput.*, 27(6):2077–2097, 2006.

[345] Gabriel Wittum. On the convergence of multi-grid methods with transforming smoothers. *Numer. Math.*, 57(1):15–38, 1990.

[346] W. Zulehner. A class of smoothers for saddle point problems. *Computing*, 65:227 – 246, 2000.

[347] W. Zulehner. Analysis of iterative methods for saddle point problems: a unified approach. *Math. Comp.*, 71:479 – 505, 2002.

[348] W. Zulehner. Uzawa-type methods for block-structured indefinite linear systems. SFB-Report 2005-5, SFB F013, Johannes Kepler University Linz, Austria, 2005.

2.2 List of abbreviations

SFB: Spezialforschungsbereich 013 (Numerical and Symbolic Scientific Computing)
Johannes Kepler Universität Linz
Hochschulfondsgebäude HF 235
Altenberger Straße 69
A-4040 Linz, Austria
`http://www.sfb013.uni-linz.ac.at`
Director: Univ. Prof. Dr. Peter Paule

RISC: Research Institute for Symbolic Computation
Johannes Kepler University
Altenberger Straße 69
A-4040 Linz, Austria
`http://www.risc.uni-linz.ac.at`
Director: Univ. Prof. Dr. Franz Winkler

RICAM: Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenberger Straße 69
A-4040 Linz, Austria
`http://www.ricam.oeaw.ac.at` Director: Prof. Dr. Heinz W. Engl

NuMa: Institute of Computational Mathematics
Johannes Kepler University Linz
Altenberger Straße 69
A-4040 Linz, Austria
`http://www.numa.uni-linz.ac.at`
Director: Univ. Prof. Dr. Ulrich Langer

Geo: Institut für Angewandte Geometrie
Johannes Kepler University
Altenberger Straße 69
A-4040 Linz, Austria
`http://www.ag.jku.at`
Director: Univ. Prof. Dr. Bert Jüttler

IndMath: Industrial Mathematics Institute
Johannes Kepler University Linz
Altenberger Straße 69
`http://www.indmath.uni-linz.ac.at`
Director: Univ. Prof. Dr. Heinz W. Engl

JKU: Johannes Kepler University Linz
Altenberger Straße 69
`http://www.jku.at`
Rector: Univ. Prof. Dr. Rudolf G. Ardelt