Abstracts of Ph.D. theses in mathematics

Commentationes Mathematicae Universitatis Carolinae, Vol. 46 (2005), No. 1, 179--195

Persistent URL: http://dml.cz/dmlcz/119518

ABSTRACTS OF Ph.D. THESES IN MATHEMATICS

defended recently at Charles University, Prague

SPATIAL IMAGINATION DEVELOPMENT OF THE SECONDARY SCHOOL PUPILS

LEISCHNER Pavel, Department of Mathematics Education, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic

(April 5, 2004; supervisor L. Boček)

In the first place the paper includes research of the thinking processes proceeding in consciousness of the pupils (in the age-bracket 15-19 years) when they settle a certain type of stereometric problems. This particularly concerns the detection of the phenomena characterising this type, knowledge of strategies of the pupils settling the issue, possibly the mechanisms, the identification of obstacles and looking for method to overcome them. The basic types of strategies and comparison of the spatial thinking level of grammar school pupils in terms of their specialisation and age are given. This in particular concerns knowledge of the difference between the pupils of the mathematical and general specialisation of the same age and between the pupils of various age at schools of the same specialisation (to determine, how a spatial imagination of the pupils of the same specialisation differs before and after teaching of stereometry).

Next part is the research of the possibilities of the application of tools of dynamic geometry in development of the spatial thinking. There are included some examples of suitable aids for teaching of stereometry with the support of Cabri geometry, the comparison of the pros and cons of these interactive aids with conventional 3D aids and the proposals of self-help production of the new 3D aids.

The last section deals with methodical suggestions for development of the spatial thinking of mathematically gifted secondary school pupils in the field of special-interest mathematics.

DIAGNOSTICS AND SENSITIVITY OF ROBUST MODELS

MAŠÍČEK Libor, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic

(April 5, 2004; supervisor J.Á. Víšek)

The thesis deals with the Least Weighted Squares estimator (LWS) which is defined as

$$\hat{\beta}^{(LWS)} = \arg\min_{\beta} \sum_{i=1}^{n} w_h \, r^2_{(h)}(\beta)$$

where $r^2_{(h)}(\beta)$ are order statistics of squared residuals in the classical regression meaning and w_h are given weights. This estimator was proposed by Víšek (2000a,b) and it generalizes the classical Least Trimmed Squares (LTS) proposed by Rousseeuw (1984).

The first part contains basic properties of the LWS estimator. Namely its breakdown point is expressed. The estimator is rewritten into the form of a statistical functional and several forms of normal equations are expressed.

In the second part there are the main theoretical results of the thesis. Namely the $\sqrt{n}$-consistency and the asymptotic normality of the LWS estimator are proved. Next the forms of the most efficient, most B-robust and most V-robust LWS estimators are deduced. Finally the common algorithms for the LTS and LWS estimators are summarized and the $\sqrt{n}$-consistency and the asymptotic normality of the basic iteration algorithm are proved.

The appendix contains examples of the LWS estimator applied to several datasets. The enclosed CD contains implementations of the algorithms for the programs Mathematica and MATLAB.

References

Rousseeuw P.J. (1984), *Multivariate Estimation with High Breakdown Point*, Proceedings of the 4th Pannoian Symposium on Mathematical Statistics and Probability, Tatzmannsdorf, Austria.

Víšek J.Á. (2000a), *On the diversity of estimates*, Comp. Stat. & Data An. **34** (67–89).

Víšek J. A. (2000b), *Regression with high breakdown point*, ROBUST'2000, J. Antoch a G. Dohnal, Eds., JČMF, 324–356.

MODERN METHODS FOR SOLVING LINEAR PROBLEMS

DUINTJER TEBBENS Erik Jurjen, Department of Numerical Mathematics,
Faculty of Mathematics and Physics, Charles University, Sokolovská 83,
186 75 Prague 8, Czech Republic
(May 19, 2004; supervisor J. Zítko)

In the present thesis we show that we can accelerate the convergence speed of restarted GMRES processes with the help of rank-one updated matrices of the form $\mathbf{A} - by^T$, where $\mathbf{A}$ is the system matrix, b is the right-hand side and y is a free parameter vector. Although some attempts to improve projection methods with rank-one updates of a different form have been undertaken (for example in Eirola, Nevanlinna [1] or in Weiss [3] and Wagner [2]), our approach, based on the Sherman-Morrison formula, is new. It allows to solve a parameter dependent auxiliary problem with the same right-hand side but a different system matrix. Regardless of the properties of $\mathbf{A}$ we can force any convergence speed of the second system when the initial guess is zero. Moreover, reasonable convergence speed of

the second system is able to overcome stagnation of the original problem. This has been tested on different kinds of problems from practice. The computation of the parameter vector $y \in \mathbb{R}r^n$ as well as computations with the rank-one updated matrix add only little costs to the restarted method.

When the initial guess is nonzero (for example at the end of restart cycles), we minimize residual norms over all possible parameter vectors. Stepwise minimization does not seem lucrative, but theoretical investigation of global minimization shows that we can project implicitly on subspaces of a dimension twice as large as the iteration number. In addition, we combine stepwise minimization with a preconditioning technique with the help of updated matrices of the form $\mathbf{A} - \mathbf{A}dy^T$ for some $d \in \mathbb{R}^n$. In numerical experiments it proved to be able to overcome stagnation of restarted GMRES.

We have also worked out results about the spectrum of the rank-one updated matrix. In theory, one can create any spectrum of $\mathbf{A} - by^T$ by the choice of the parameter vector $y \in \mathbb{R}^n$. In practice it is only feasible to prescribe Ritz values of the auxiliary matrix. But when we assume we have a nearly normal matrix also modification of selected eigenvalues can be achieved. Based on these ideas, we have constructed algorithms for both normal and nonnormal matrices. In problems where spectral properties hampered convergence, these techniques could accelerate the GMRES process.

References

[1] Eirola T., Nevanlinna O., *Accelerating with rank-one updates*, Linear Algebra Appl. **121** (1989), 511–520.

[2] Wagner B., *Kurze Rekursionen bei präkonditionierten CKS-Verfahren*, Internal report 54/95, University of Karlsruhe, Computer center, Postfach 6980, D-76128 Karlsruhe, Germany, 1995. Diploma thesis.

[3] Weiss R., *Minimization properties and short recurrences for Krylov subspace methods*, Electronic Transactions on Numerical Analysis (ETNA) **2** (1994), 57–75.

NUMERICAL REALIZATION OF TRUST REGION METHODS

MATONOHA Ctirad, Department of Numerical Mathematics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic

(May 19, 2004; supervisor J. Zítko)

This work deals with trust region methods for local optimization problems. Optimization means minimization or maximization of an objective function with or without constraints on variables. Such constraints may be equalities, inequalities or both. Trust region methods have an iteration character, where determination of a direction vector is a key problem. Since such a vector is found iteratively, an inner iteration cycle is obtained. We construct a simple model of the objective function (quadratic approximation) in a neighbourhood of a current point and

seek a minimum of this model. Thus, trust region methods determine the direction vector by solving a minimization subproblem with a quadratic function on some region, e.g. sphere.

Most trust region methods lead to system of linear equations, which is unsuitable mainly for large scale optimization problems. However, there exist iteration methods with subsequently generated Krylov subspaces having a special structure that allows us to solve this subproblem efficiently. Another access to determining the direction vector is based on a transformation of the main subproblem to the parametric eigenvalue problem. In all cases the optimal or approximating solution satisfying the optimality conditions is obtained.

An overview and a theory of the trust region methods are given. Individual types of methods, their basic properties and algorithms as well as new algorithms for unconstrained optimization and original proofs of global convergence are introduced. Numerical comparisons of all methods on various types of testing problems are also performed.

The last chapter is about using the trust region methods in interior point methods for general constrained minimization. Interior point methods are an effective tool for solving general nonlinear programming problems, especially for large scale structured problems. The application of the trust region methods for general constraints and using the so called filter technique instead of the penalty function for a stepsize selection are original results of this work. New constructed algorithms are tested and compared on various types of testing problems.

DELTA CONVEXITY, METRIC PROJECTION AND NEGLIGIBLE SETS

DUDA Jakub, Department of Mathematical Analysis, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(June 2, 2004; supervisor L. Zajíček)

This thesis consists of five chapters, each of which corresponds to a paper: *On inverses of δ-convex mappings*, Comment. Math. Univ. Carolinae **42**, no. 2 (2001), 281–297; *On d.c. functions and mappings*, joint work with L. Veselý, and L. Zajíček, Atti Sem. Mat. Fis. Univ. Modena **51** (2003), 111–138; *On the size of the set of points where the metric projection exists*, Israel J. Math. **140** (2004), 271–283; *Curves with finite turn*, submitted[1]; *On a decomposition of superreflexive spaces*, submitted[1].

The first chapter answers three questions concerning stability of d.c. mappings posed by Veselý, and Zajíček. A mapping $F : \Omega \subset X \to Y$ (X, Y are normed linear spaces, Ω an open convex set) is called *d.c.* (or *delta-convex*) if there exists a continuous function $f : \Omega \to \mathbb{R}$ so that $y^* \circ F + f$ is continuous and convex for each $y^* \in Y^*$ with $\|y^*\| = 1$. We construct a bilipschitz surjective d.c. map $N : \ell_1 \to \ell_1$ so that N^{-1} is nowhere locally d.c. (a slight modification of the

[1]Available at `http://www.karlin.mff.cuni.cz/kma-preprints`.

construction allows us to construct such a mapping so that N is even strictly differentiable at some point). This shows that an inverse of a bilipschitz d.c. map can fail to be locally d.c. at any point.

The second chapter consists of two parts. The first is an up-to-date survey of results about d.c. functions and mappings. The second part contains new results. For example, we prove that for each Banach space Y, every $C^{1,1}(\Omega; Y)$-map ($\Omega \subset X$ convex) is d.c. if and only if X has an equivalent norm with modulus of convexity of power type 2. We also prove that if X is an Asplund space, and there exists a bilipschitz d.c. mapping between two open convex sets $A \subset X$, and $B \subset Y$, then X and Y are linearly isomorphic.

In the third chapter, we resolve two conjectures of J.P.R. Christensen. He conjectured that, in a separable reflexive space, the nearest points to a closed set exist almost everywhere (i.e. outside of a Haar null set). He also made another conjecture concerning the differentiability of the distance function, which can be reduced to the previous conjecture via a theorem of Fitzpatrick. Using a decomposition of ℓ_2, by Matoušek and Matoušková, into a ball small set and Aronszajn null set, we provide a counterexample. V. Zizler (private communication) asked the same question for farthest points. We also provide a counterexample in this situation.

The fourth chapter is dedicated to the study of curves with finite turn (resp. curves with finite turn of tangents). These were studied by Pogorelov (in $\mathbb{R}^3$), and by Alexandrov, and Reshetnyak (in $\mathbb{R}^n$). We generalize these notions to curves with values in an arbitrary Banach space, and prove that they are equivalent. Further, we prove several results about the relation of curves with finite turn, and of delta-convex curves. This allows us to generalize some results of Alexandrov, Reshetnyak, and Pogorelov.

In the last chapter, we study decompositions of certain super-reflexive spaces into ball-small sets (notion due to Preiss and Zajíček), and Aronszajn null sets. The main result is that if X is an infinite-dimensional Banach space with modulus of convexity of power type p, then there exists a Borel set $A \subset X$ which is ball-small, and whose complement is Aronszajn null. This generalizes a result of Matoušek and Matoušková, who constructed such a decomposition of a separable Hilbert space. As a corollary, we obtain that Christensen's conjecture is false in such spaces.

CHOQUET'S THEORY IN FUNCTION SPACES

SMRČKA Michael, Department of Mathematical Analysis, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(June 2, 2004; supervisor J. Lukeš)

In this work we study some possibilities of the transfer of the notions, theorems and instruments of proofs from the convex theory to the theory of the function

spaces. This is the main aim of this work.

If the source notion in the convex theory is the notion of the face then the corresponding notion in the theory of function spaces is the Choquet set.

There exists a large monograph (E.M. Alfsen, Compact convex sets and boundary integrals, Springer-Verlag, 1971) which treats the structure of a compact convex set in a locally convex space. During the more than thirty years since the book was issued, many problems were solved but other remained without an answer.

In the first chapter we introduce basic notions of the Choquet's theory.

The barycentre of the second chapter is the definition and the study of the Archimedean set. Here we had two possibilities of the further progress. The first of them was to use the notion of the state space which represents "a bridge" between the theory of the local convex spaces and the Choquet theory of the function spaces. We chose the second possibility, i.e. to use "inner" properties of the function spaces.

The starting point is the M-set whose implementation is not unique in the bibliography. We give several equivalent expressions of this notion.

In the third chapter we give an application to potential theory. The original idea was to use a facial topology for the exploration of the space of harmonic functions, especially for solving the Dirichlet problem. In this direction we were disappointed a bit: in the case when the set of regular points is not closed the only facially continuous functions are the constants.

In the fourth chapter we pay attention to two notions mainly, the measure convexity and A(K)-extremality.

SEARCH PROBLEMS AND BOUNDED ARITHMETIC

HANIKA Jiří, Department of Applied Mathematics, Faculty of Mathematics and Physics, Charles University, Malostranské nám. 25, 118 00 Prague 1, Czech Republic

(June 28, 2004; supervisor J. Krajíček)

We study search problems and reducibilities between them with known or potential relevance to bounded arithmetic theories. Our primary objective is to understand the sets of low complexity sequences (esp. Σ^b_1 or Σ^b_2 of theories S^i_2 and T^i_2 for small i, ideally in a rather strong sense of characterization; or, at least in the standard sense of axiomatization). We also strive for maximum combinatorial simplicity of the characterizations and axiomatizations eventually sufficient to prove conjectured separation results. To this end, two techniques based on the Herbrand's theorem are developed. They characterize/axiomatize Σ^b_1-consequences of Σ^b_2-definable search problems, while the method bases on the more involved concept of characterization is easier and gives more transparent results. This method yields new proofs of Buss' witnessing theorem and of the relation between PLS and Σ^b_1 (T^1_2), and also an axiomatization of Σ^b_1 (T^2_2). We also investigate the

relations among known search problems such as GI, MIN and GLS and some of their variants.

ASYMPTOTICS IN STOCHASTIC GEOMETRY

PAWLAS Zbyněk, Department of Probability and Mathematical Statistics,
Faculty of Mathematics and Physics, Charles University, Sokolovská 83,
186 75 Prague 8, Czech Republic
(September 8, 2004; supervisor V. Beneš)

Stochastic geometry is a field of mathematics based on probability theory and integral geometry (see [5]). The main aim of this thesis is to investigate the asymptotic behaviour of stochastic geometric models observed through a bounded window W_n which expands without bound in all directions as $n \to \infty$.

Randomly placed random compact subsets of the d-dimensional Euclidean space form a particle process. In the first part, which is based mainly on the original papers [4] and [3], we study a random measure generated by a translation invariant measure ζ. It is defined as the total ζ-measure of a stationary particle process. The central limit theorem for a usual intensity estimator is formulated. In the Poisson case we derive the rates of normal convergence. An application of the central limit theorem contains the construction of asymptotic confidence intervals.

Special attention is devoted to the Poisson segment process. Asymptotic variances of two basic length intensity estimators are compared. It is shown that Theorem 4 in [2] follows under weaker assumptions on the segment process and the observation window and that it can be generalized to higher dimensions and more general processes. We present a simulation study which is used to illustrate the results.

The second part comes from a joint work with Lothar Heinrich [1]. We consider an m-dimensional functional describing basic properties of individual particles of the process. The appropriately weighted empirical counterpart of the corresponding distribution function is introduced. We prove a Glivenko-type theorem and the weak convergence of the multivariate empirical process in the Skorohod space $D(\mathbb{R}^m)$. Consequently, a Kolmogorov-Smirnov test can be established in the one-dimensional case provided that the distribution function is continuous.

References

[1] Heinrich L., Pawlas Z. (2004), *Weak and strong convergence of empirical distribution functions in germ-grain models*, in: Spatial Point Process Modelling and Its Applications, A. Baddeley, P. Gregori, J. Mateu, R. Stoica and D. Stoyan (eds.), pp. 101–124. *Statistics, submitted.*

[2] Mrkvička T. (2001), *Estimation variances for Poisson processes of compact sets*, Adv. in Appl. Probab. **33** (765–772).

[3] Pawlas Z. (2003), *Central limit theorem for random measures generated by stationary processes of compact sets*, Kybernetika **39**, 719–729.

[4] Pawlas Z., Beneš V. (2004), *On the central limit theorem for the stationary Poisson process of compact sets*, Math. Nachr. **267**, 77–87.

[5] Stoyan D., Kendall W.S., Mecke J. (1995), *Stochastic Geometry and Its Applications*, 2nd edition, Wiley, New York.

METHODS OF STEREOLOGY AND SPATIAL STATISTICS IN APPLICATIONS

BODLÁK Karel, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(September 15, 2004; supervisor V. Beneš)

This work is oriented on the theory and methods of spatial statistics where we want to suggest new methods for solving particular problems in the field of point processes and stereology. Computer modeling of point systems has become an important tool in many fields of research and also in manufacturing. Typically simulations help to describe the relationship between variables studied and try to measure variability and random effects in mathematical models. We study the flexible class of Log Gaussian Cox point processes where it is possible to include additional deterministic information in covarites. The extended model of this process may be used for modeling of various situations in econometrics where spatial information is involved in the data. Furthermore, the epidemiological application on the tick disease is done. For this purpose Bayesian MCMC technique is studied in order to be able to deal with posterior characteristics in the suggested model.

The stereological method of unfolding is one of widely applied methods in material science. Here we developed numerical solution of bivariate size-orientation unfolding for platelike particles. It concerns the design of a discrete setup for the numerical method and application of the EM algorithm. The quality of the suggested method is tested on synthetic examples, where we know two- and three-dimensional bivariate size-orientation distributions. Further, the proposed method is employed on the estimations of bivariate three-dimensional size-orientation distributions of microcracks which reflect crack behaviour under compressive and tension deformation in aluminium alloys.

Inspired by the extreme value theory we studied the conditional and marginal distribution of the extreme of a shape factor which can be estimated. The starting point is the classical size-shape unfolding for spheroidal particles, especially oblates. The idea is based on the fact that the planar and the spatial distribution under certain conditions belong to the same domain of attraction. It means we can predict estimates of extremes in the space from extremes in planar measurement. The applicability of the suggested method is verified on the simulation study.

M-SMOOTHERS

ČAPEK Václav, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(September 15, 2004; supervisor M. Hušková)

The topic of the thesis is M-smoothers. We chose it as it is quite new and has a number of possible applications in various scientific fields.

We propose an application of a bootstrap method in the setup of M-smoothers. We start from a theorem proved in Antoch and Janssen (1989), and show that a properly chosen bootstrap procedure provides reasonable approximations of the limit distribution of the M-smoother. We believe that such estimation can be easily applied in real data problems — among the possible applications of our method, there is an evaluation of critical values for different types of tests.

Further, we use the results on M-smoothers to develop a test of continuity of a regression function, as we know that the assumption of continuity of a regression function is not met in a number of real examples. We consider a test at a specified point and also a global test. In case of the test at a specified point we derive a limit distribution of our test statistics under the null hypothesis. We show consistency of this test and, moreover, that the critical values can be approximated using a bootstrap method. In case of the global test we show its consistency.

To prove the results we use common methods of probability and asymptotic statistics, such as the Lyapunov central limit theorem for triangular arrays or the Bernstein inequality.

Finally we check how our procedures work on simulated data. Moreover, we apply our methods to the Klementinum data. We plan to study the Klementinum data more in detail and propose extensions of our methods to be applied to this data.

PREDICTION IN NON-LINEAR AUTOREGRESSIVE PROCESSES

ZVÁRA Petr, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(September 15, 2004; supervisor J. Anděl)

In this work, the problem of prediction in the autoregressive time series data is discussed. Both linear autoregression (AR) and non-linear autoregression (NLAR) mainly of order 1 with positive noise are studied. We discuss the setup when all parameters are known and when the autoregression parameters remain unknown as well. Some results for the multivariate general order processes are presented.

In Chapter 2, the linear autoregressive time series models and the prediction problem are introduced and the relevant results are summarized. The 1-step and 2-step ahead prediction in NLAR processes is studied in the second section of

Chapter 2. In Chapter 3, we consider more realistic setup when the autoregressive parameters are unknown and must be estimated. The effect of parameter uncertainty on prediction is analysed. The problems of point and interval prediction as well as coverage probability issues are discussed. In Chapter 4, we deal with the non-linear multidimensional NLAR(p) processes. The time series model for the compositional data is introduced. Procedures used for numerical computations of predictions and stationary distributions are described in Appendix A.

PRICING OF LIFE INSURANCE PRODUCTS

BLANDA Jiří, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(September 16, 2004; supervisor P. Mandl)

The aim of the thesis is the pricing of life insurance products using stochastic models. The thesis consists of four chapters. In the first chapter, some basic terms from the theory of contingent claims pricing are introduced, for instance the generalized Black-Scholes option pricing formula and the Heath-Jarrow-Morton interest-rate model. In Chapter 2, a theory for pricing the unit-linked life insurance products with guarantee is presented. In Chapter 3, a pricing model for the traditional endowment insurance is developed. In both chapters, the pricing of life insurance products is initially based on a basic model. In this model, the interest rate is constant and the price of risky asset follows a geometric Brownian motion. The model is subsequently extended taking into account the term structure of interest rates. In Chapter 4, some pros and cons of the presented approach are discussed.

The contingent claims pricing theory provides a basis for pricing of life insurance products, as well as for the value-based management of an insurance company. Historic approaches are usually insufficiently accurate to enable companies to achieve value maximising goals reliably in a competitive market environment.

MODEL FOR CALCULATION OF LIABILITY VALUE ARISING FROM LIFE INSURANCE

FINFRLE Pavel, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(September 16, 2004; supervisor P. Mandl)

The fair value is broadly considered being the future of reporting the insurers economic situation. However, except some accepted general sentences, there is no consensus about the real definition of the fair value and approaches to its calculation.

The model is inspired by the complex approach described by Steffensen (2002).

However, we disagree with some basic prerequisites of the Steffensen approach, since there is obvious evidence that the primary market is far from being arbitrage-free. Consequently, we have to disagree with usage of option model for policyholder behavior modeling.

We assume fictive arbitrage-free secondary market of policies. Similarly to the real insurers approach, the secondary market participants would approach the exercises of policyholders options as not being determined by the state of secondary market state, but just influenced. Therefore, we calculate the fair value as the conditional expectation of discounted policy cash flow under the risk neutral probability measure corresponding to secondary market of policies and conditional to the state of the secondary market. It allows us to avoid the necessity of assessing policyholder preferences when modeling the lapses and, subsequently, to decrease sharply the complexity of the model. Moreover, we are convinced that this way of thinking corresponds to the real insurers approach to its portfolio.

References

[1] Steffensen M., *Intervention options in life insurance*, Insurance Math. Econom. **31** (2002), no. 1, 71–85.

ORTHONORMAL WAVELETS AND THEIR APPLICATIONS

FINĚK Václav, Department of Numerical Mathematics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(September 24, 2004; supervisor K. Najzar)

In many wavelets' applications, the scalar product of a given function with the scaling function has to be calculated. For deriving effective wavelet based one-point quadrature formulas, the relation between the first scaling moments and the second one is crucial. And this was a motivation to try to find further relations.

First, we prove the validity of additional relations among scaling moments for orthonormal scaling functions with some polynomial exactness and in general with noncompact support. Further, we derive a new orthonormality condition for scaling functions with compact support. This condition shows a close connection between orthonormality of the scaling functions and relations among discrete scaling moments. Then again with some polynomial exactness we prove the validity of further relations among scaling moments. (Strictly speaking for the scaling functions with compact support we are able to find two times more relations.)

Furthermore, anti-derivatives of scaling function of Daubechies' wavelets are employed to solve two-point boundary value problems, quadrature formulas based on the scaling function corresponding to Daubechies wavelet with two vanishing moments are proposed and, finally, methods of computation of scaling coefficients of Daubechies' wavelets are reviewed and a new one is proposed.

LEFT DISTRIBUTIVE LEFT QUASIGROUPS

STANOVSKÝ David, Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(October 7, 2004; supervisor J. Ježek)

We study *left distributive left quasigroups* (known also as racks or quandles) and their connection to other algebraic structures, such as groups and weakly associative loops. They are binary algebras satisfying the identity

$$x(yz) = (xy)(xz)$$

and the property

$$\text{for every } \ a,\, b \ \text{ there is a unique } \ c \ \text{ with } \ ac = b.$$

There is a very natural example: on a group G, define a new operation by $a * b = aba^{-1}$. It turns out that the set G with the operation $*$ is a left distributive left quasigroup.

In the first chapter, we study the subvariety of left symmetric left distributive idempotent groupoids in detail. Basic properties of this variety are described and, particularly, a correspondence between such groupoids of odd exponent and the well-known class of Bruck loops is found. The next chapter contains a new solution of the eighth Belousov's problem: the smallest left distributive quasigroup which is not isotopic to any Bol loop is found. Further, we study the equational theory of group conjugation; we look for its basis and we prove several properties of the corresponding variety. In the next chapter, we describe non-idempotent subdirectly irreducible left distributive left quasigroups and, finally, we show a couple of properties of subvarieties of the variety of left distributive left idempotent groupoids.

The thesis contains also a thematically independent appendix, which deals with the following problem: which algebras are homomorphic images of subdirectly irreducible algebras? We present a solution for algebras with at least one at least binary operation.

POLYHEDRA AND SECONDARY SCHOOL MATHEMATICS

KOBLÍŽKOVÁ Michaela, Department of Mathematics Education, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(October 21, 2004; supervisor J. Kadleček)

The thesis consists of two independent parts: In the first part reasons are given for general conception, destination and methodical approach to the latter part, which is the book Let Us Get Insight into Polyhedra, a collection of solved problems from the field of solid geometry.

Each part of thesis is fully independent. It has its own contents, bibliography and paging. The book connects secondary school level of mathematical knowledge with tasks of Mathematical Olympics. It is meant for self-studying. The author has done her best to reach the largest extent of problems included.

The book consists of thirteen chapters: 1. Do you really know the cube?; 2. Simple and perfect body; 3. Pyramids, prisms, polyhedra; 4. Euler's theorem and types of polyhedra; 5. Regular tetrahedron and cube have only three more members of the family; 6. Another polyhedra with regular faces; 7. Polyhedra sharing given property; 8. Cuts and intersections; 9. Nets of polyhedra and how we can use them; 10. Sorting and describing convex polyhedra; 11. Rotation and colouring of polyhedra; 12. Further problems; 13. Historical and other matters of interest.

Every chapter of the book consists of one or two pages introducing problems and several pages of theirs solutions. The main achievement is always repeated and precised in the end of the chapter.

There are more than one hundred drawings included in the book. Geometry is shown to be not only very attractive part of mathematics but also very useful for practising other mathematical skills.

INVARIANT DIFFERENTIAL OPERATORS FOR PROJECTIVE CONTACT GEOMETRIES

KRÝSL Svatopluk, Mathematical Institute, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(October 25, 2004; supervisor V. Souček)

The main topic of this dissertation thesis is a study of invariant differential operators on projective contact manifolds.

Contact manifolds are an arena of time-dependent mechanics. The projective contact geometry can be packed into the realm of Cartan geometries — some additional data (projective equivalence class of contact connections) are needed. On the other hand, there are some quantum mechanical systems which are described by fields with values in the so called Segal-Shale-Weil (or symplectic spinor) representations of the metaplectic group, a double cover of the symplectic group. These representations ware studied by B. Kostant (among others) with the intention of generalizing the classical Dirac operator to the symplectic case.

We have defined so called harmonic module which is a proper analog of the spinor-tensor in the orthogonal case, i.e., a harmonic module is an irreducible component of the tensor product of the symplectic spinor module with a finite dimensional representation of the symplectic Lie algebra.

We have classified all first order invariant differential operators acting between sections over manifolds with a given projective contact structure having their values in the harmonic modules. In this part we needed to generalize some results on decomposition of the tensor product of the symplectic spinor representation

and a finite dimensional representation to the case of the tensor product of a harmonic module and the defining representation of the symplectic Lie algebra.

Further, we investigated the so called Bernstein-Gelfand-Gelfand (BGG) and Hasse diagrams for finite dimensional representations of the contact graded symplectic Lie algebra. In the thesis, some transformation formulas for projective contact geometry (e.g., for contact connections and contact projections) were derived and the behavior of the homogeneous model was investigated with respect to these transformations. In the thesis, the BGG and Hasse diagrams for contact graded orthogonal algebras of odd rank are described explicitly.

PROPERTIES OF INVARIANT DIFFERENTIAL OPERATORS

ŠMÍD Dalibor, Mathematical Institute, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(October 25, 2004; supervisor V. Souček)

The thesis deals with the topic of differential operators acting between various vector bundles over a given manifold. More specifically, we consider operators acting on homogeneous bundles given as $G \times_H \mathbb{V}$, where G is a semisimple Lie group, H its subgroup, and $\mathbb{V}$ an irreducible H-module. Operators intertwining the action of a representation of G on the set of sections of these bundles are called invariant. We deal with two types of H — either it is a parabolic subgroup of G, or it is its maximal compact subgroup. In the former case, there is a well established theory that classifies the so called standard operators in the language of Bernstein-Bernstein-Gelfand sequences. In the case of a complex group G, these are parameterised by G, H and a G-dominant weight, their shape does not depend on the weight. In the case of bundles associated to a homogeneous space they are complices, i.e. the composition of any two subsequent operators is zero. The theory of BGG sequences works and the related algebraic machinery works however for the more general case of parabolic geometries too. In the case of H maximal compact, i.e. G/H a symmetric space, the number of invariant differential operators is considerably higher and there is also no theory of curved analogs as in the parabolic case.

There are two problems studied in the thesis. The first one is a complete classification of invariant differential operators for the parabolic geometry given by the standard contact gradation of even-dimensional complex orthogonal Lie algebras and their real forms. It engages well-known algorithms but the result is completely general, non-algorithmical. The second problem is a generalisation of a remarkable theorem of Ørsted on intertwining invariant differential operators in a symmetric space with the operators on the parabolic geometry that can be viewed as its boundary. A theorem establishing this intertwining for standard operators of arbitrary order is the main result of the second part of the thesis. The tool is the so called Poisson transform and the possible application can include a better

insight into the AdS/CFT correspondence of theoretical physics or to the ambient metric construction of invariant differential operators.

NOTES ON APPROXIMATION OF STOCHASTIC PROGRAMMING PROBLEMS

ŠMÍD Martin, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(November 10, 2004; supervisor V. Kaňková)

Since many "real-life" stochastic programming problems lack an analytic solution, they have to be approximated. Three different methods of stochastic programming problems (SPP) approximation are examined and compared in the thesis: the discretization (i.e. the replacement of the random parameter's distribution by a discrete one), the Monte Carlo (i.e. the replacement of the value function's expectation by the average of an i.i.d. sample) and a special method consisting in a combination of the discretization and the Monte Carlo (we call it Quasi Monte Carlo[2]). The main criterion of the comparison is the convergence rate of the approximation error.

The discretization is widely used to approximate SPPs and a large amount of literature has been devoted to this technique. It is known that an SPP with the value function Lipschitz in the chance parameter and with bounded support of the chance parameter may be discretized so that the approximation error is $O(n^{-1/k})$ (n is the number of atoms of the approximating distribution and k is the dimensionality of the chance parameter). The thesis generalizes this result for the case of an unbounded support of the chance parameter and for the multistage problems.

Also the Monte Carlo approximation has been widely studied: various bounds of the approximation error have been introduced and the convergence rate $O(n^{-1/2})$, where n is the size of the Monte Carlo sample, has been proved for the case of a one-stage SPP with unique minimizer. The thesis generalizes this result for multiple optimal solutions and it evaluates the convergence rate of the Monte Carlo approximation in case that the SPP problem is multistage.

The third technique — Quasi Monte Carlo — was suggested to compute a volume of multi-dimensional bodies and it has not been used for the stochastic programming problems approximation yet. The thesis provides a convergence rate of the Quasi Monte Carlo both for the one-stage and for the multistage problems.

[2]To avoid possible misunderstanding, it should be stressed here that the name Quasi Monte Carlo is being used for a wide range of approximation techniques, not only for the one studied in the thesis.

CHANGE POINT PROBLEM FOR CENSORED DATA

KOMÁRKOVÁ Lenka, Department of Probability and Mathematical Statistics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(December 8, 2004; supervisor M. Hušková)

The thesis deals with the problem of a detection of a change (changes) in the distribution of survival variables that are independent but possibly censored. We consider not only the change in the distribution of the survival variables but also the change in the distribution of the censoring variables which complicates the problem. The work extends the results recently given by Hušková and Neuhaus (2004). We focus on the test and estimate procedures based on ranks. The test statistics and corresponding estimators are derived using the same principle as for uncensored data. We consider max-type test statistics applied to one-change problem and MOSUM-type rank statistics suitable for testing multiple changes. The limit behavior for such classes of test statistics under the hypothesis of "no change" in the distribution of censored data is studied. Particularly, under equal censorship, the permutation principle can be used. Moreover, the consistency of our test procedures is proved. Further, two classes of estimators of the change point corresponding to the max-type test statistics are proposed and their limit properties (namely the rate of consistency and the limit distribution under the hypothesis) are investigated. The theoretical results are accompanied by quite extensive simulations based on the Monte Carlo repetitions or on the bootstrap without replacement.

References

[1] Hušková M., Neuhaus G., *Change Point Analysis for Censored Data*, J. Statist. Plann. Inference **126** (2004), no. 1, 207–223.

COMMUTATIVE ALGEBRA AND CRYPTOGRAPHY

KECHLIBAR Marian, Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
(December 13, 2004; supervisor T. Kepka)

The thesis is divided into three parts, covering distinct fields of research.

The first part concerns generalization of the Units Theorem to factors of polynomial rings (affine variations). The author shows usage of homogenization and localization techniques in order to prove the following commutative algebraic theorem:

> Let k be a field and $R = k[x_1, \ldots, x_l]$ a finitely generated domain over it; let k' denote the algebraic closure of k in R. Then the group R^*/k'^* is finitely generated.

The second part is also concerned with finitely generated objects. The author concentrated on properties forcing semilocal commutative rings (that is, rings with finitely many maximal ideals) to be finite. With use of number theory, theory of radical rings and Baer theory of minimax groups, many assertions on finiteness and infinity of semilocal rings are proved, with the most significant ones being:

Every finitely generated semilocal ring is finite.

Let R be semilocal and R^* finitely generated. Then R is finite.

Let R be semilocal and R^* or $R(+)$ be minimax. Then R is finite.

The third part of the thesis analyses the Quadratic Sieve factoring algorithm, from both theoretical and implementation point of view. It demonstrates several nontrivial properties of the QS algorithm, regarding ranks of bit matrices used during the process, with the most noticeable and never-before observed problem of the "Singleton Gap".