

Forschungsbericht 2008

Institut für Algebra und Geometrie



Otto-von-Guericke-Universität Magdeburg

Fakultät für Mathematik

Institut für Algebra und Geometrie

Universitätsplatz 2, 39106 Magdeburg
Tel. +49 (0)391 67 18713 / 18321, Fax +49 (0)391 67 11213
kerstin.held@ovgu.de oder
jeannette.polte@ovgu.de

1. Leitung

Prof. Dr. Alexander Pott (geschäftsführender Leiter)

Prof. Dr. Wolfgang Willems

Jun.-Prof. Dr. Christian Bey (ab 01.10.2008 Vertretungsprof. W2-Algebra)

Dr. Achill Schürmann

2. Hochschullehrer

Juniorprofessor Dr. Christian Bey (ab 01.10.2008 Vertretungsprof. W2-Algebra)

Prof. Dr. Heidemarie Bräsel

Prof. Dr. Martin Henk

Prof. Dr. Herbert Henning

Prof. Dr. Alexander Pott

Prof. Dr. Wolfgang Willems

3. Forschungsprofil

Didaktik der Mathematik

- Theoretische und empirische Untersuchungen zu Niveaustufungen bei der Herausbildung von Modellbildungskompetenzen im Mathematikunterricht der Klassen 9 und 12
- Untersuchungen zur Umsetzung von Bildungsstandards in der SI und SII im Rahmen des Forschungsprojektes "Aufgabenvariation im Mathematikunterricht"
- Sprache und Mathematik
- Kompetenzentwicklung und Niveaubestimmung im mathematischen Unterricht

Diskrete Mathematik

- Untersuchung von binären Sequenzen, von Abbildungen auf endlichen Körpern sowie von Differenzmengen.
 - almost perfect nonlinear functions
 - Bent-negabent Funktionen
 - Quadratische Potenzfunktionen
 - almost bent Funktionen
- Schedulingtheorie
 - Strukturuntersuchung von Lösungen und Lösungsbereichen deterministischer Schedulingprobleme
 - Nachweis der Komplexität derartiger Probleme
 - Entwicklung von exakten und näherungsweise Algorithmen zu Schedulingproblemen, insbesondere unter Ausnutzung der Irreduzibilität und von Eigenschaften von Comparability-Graphen
 - Ständige Entwicklung des Softwarepaketes "LiSA - Library of Scheduling Algorithms"

Konvexe und diskrete Geometrie

- Gitterpunkte und das Ehrhart Polynom
- Nullstellen geometrischer Polynome
- Frobenius Problem

- Kompakte Darstellungen spezieller semi-algebraischer Mengen
- Extremale Gitter
- Kugelüberdeckungen
- Klassifikation perfekter Gitter
- Gleichseitige Mengen in normierten Räumen

Kombinatorik

- Diskrete isoperimetrische und -diametrische Probleme
- Kombinatorik partieller Ordnungen
- Extremale Mengentheorie

Reine Mathematik

- Codierungstheorie
 - Konstruktion optimaler Codes
 - selbstduale Codes
 - asymptotisch gute Codes
- Gruppen- und Darstellungstheorie
 - Blocktheorie für verschiedene Primzahlen
 - Quadratische Geometrien und Involutionen
 - Dualität und Morita-Äquivalenz

4. Forschungsprojekte

Projektleiter: apl. Prof. Dr. Heidemarie Bräsel

Förderer: Sonstige; 01.10.2005 - 30.09.2008

Comparabilitygraphen in der Schedulingtheorie

weitere Projektleiter: Prof. Dr. Stefan Schirra (FIN-ISG) und apl. Prof. Dr. Frank Werner (FMA-IMO)

Ein neuer Modellierungsansatz von Shop-Schedulingproblemen über eine Klasse von Comparabilitygraphen soll sowohl in theoretischer Hinsicht als auch in seiner algorithmischen Verwertbarkeit untersucht werden. Die aus dem neuen Modell abgeleiteten Verfahren sollen bezüglich Effizienz und Güte unter Nutzung des Softwarepaketes LiSA evaluiert und mit existierenden Verfahren verglichen werden.

Projektleiter: Prof. Dr. Martin Henk

Projektbearbeiter: Dr. Makato Tagami

Förderer: Sonstige; 01.04.2007 - 31.03.2008

Das Ehrhart Polynom

Wir untersuchen das Ehrhart Polynom für 0-symmetrische Gitterpolytope, und suchen nach nicht-trivialen unteren Schranken für seine Koeffizienten. Wir erhoffen uns davon auch eine untere Schranke für das Volumen von 0-symmetrischen Polytopen in Abhängigkeit der Anzahl der inneren Gitterpunkte.

Projektleiter: Prof. Dr. Martin Henk

Projektbearbeiter: Dr. Gennadiy Averkov

Förderer: DFG; 01.03.2006 - 31.03.2009

Forschergruppe TP 2 - Darstellbarkeit und Approximierbarkeit von semi-algebraischen Mengen

In this project we study how well a given semi-algebraic set can be represented or approximated by a "simpler" semi-algebraic set. Based on the theorem of Bröcker and Scheiderer on the stability index of basic closed or open semi-algebraic sets we want to develop a hierarchical system (depending on the degree of the polynomials) of semi-algebraic sets which describe or approximate a given semi-algebraic set. As a result we expect a more compact description of semi-algebraic sets which can be gainfully used for algorithmic purposes in other projects of this

research unit.

Projektleiter: Prof. Dr. Martin Henk

Projektbearbeiter: Matthias Henze, Eval Linke, Martin Henk

Förderer: DFG; 01.05.2008 - 01.05.2011

Geometrie der Zahlen und Ehrhart Polynome

Ziel des Forschungsvorhabens ist es, Verbindungen zwischen der klassischen Geometrie der Zahlen und der neueren Theorie der Ehrhart-Polynome zu untersuchen, herzustellen und weiter auszubauen. Die zentrale mathematische Struktur in beiden Gebieten ist die Menge der Gitterpunkte (ganzzahligen Punkte) in einem konvexen Bereich.

Projektleiter: Prof. Dr. Martin Henk

Projektbearbeiter: Prof. Dr. Maria A. Hernandez Cifre

Förderer: Sonstige; 01.10.2006 - 03.08.2009

Roots of geometric polynomials

Together with Prof. Dr. Maria A. Hernandez Cifre with study the properties of the roots of two classical geometric polynomials, the Steiner and the Ehrhart polynomial.

Prof. Hernandez Cifre spent the first year at the University of Magdeburg supported by a Spanish National Grant in the programm ""Salvador De Madariaga".

We continue our investigations within the scope of the reseacrh project

Reference: MTM2007-64504

Title: Geometría diferencial y convexa: Problemas variacionales y de optimización Convex and Differential Geometry: Optimization and Variational Problems).

Institution: Universidad de Murcia

Main researcher: Luis J. Alías Linares

This is a joint project with the instiute of topology and geometry of the universiad murcia.

Projektleiter: Prof. Dr. Alexander Pott

Projektbearbeiter: Prof. Dr. Alexander Pott, Faruk Göloğlu

Förderer: DAAD; 01.10.2006 - 31.12.2009

Perfekte und fast perfekte Folgen

In der Kryptographie werden häufig binäre Funktionen benötigt, die resistent gegen lineare und differenzielle Attacken sind. Perfekte und fast perfekte Folgen sind in dieser Hinsicht optimal. Es gibt einige Klassen solcher Funktionen. Ziel des Projektes ist es, weitere Funktionen zu finden oder zu zeigen, dass es keine weiteren geben kann.

Projektleiter: Prof. Dr. Alexander Pott

Projektbearbeiter: Prof. Dr. Alexander Pott, Tan Yin

Förderer: Sonstige; 01.10.2007 - 31.03.2009

Relative Differenzmengen und Verallgemeinerungen

Das Studium relativer Differenzmengen ist sowohl von Seiten der Geometrie (projektive und affine Ebenen) als auch der Signalverarbeitung (Sequenzen mit guten Korrelationseigenschaften) von Interesse. In diesem Projekt sollen neue notwendige und hinreichende Bedingungen für die Existenz solcher Differenzmengen gefunden werden.

Projektleiter: Dr. Achill Schürmann

Förderer: DFG; 01.07.2007 - 30.06.2009

Geometrie und Algorithmik von periodischen Punktmengen

Gitter und allgemeiner periodische Punktmengen sind allgegenwärtige Objekte in der Mathematik und ihren Anwendungen. Häufig werden sie als diskrete Modelle für kompliziertere geometrische Räume verwendet. Ziel unseres Forschungsvorhabens ist es, das Zusammenspiel zwischen periodischen Punktmengen und umliegenden Räumen grundlegend zu verstehen. Im Mittelpunkt stehen dabei euklidische Räume und die Suche nach optimalen oder zumindest neuen besten periodischen Punktmengen für verschiedene geometrische Fragestellungen, wie z.B. die klassischen Kugelpackungs- und Überdeckungsprobleme. Viele dieser Probleme können als kombinatorische Optimierungsprobleme formuliert und mit Hilfe entsprechender Algorithmen und Software prinzipiell gelöst werden. Dabei spielen spezielle durch die periodische Punktmenge induzierten Zerlegungen des Raumes in Polyeder (Voronoi- und Delone-Zerlegung) eine wichtige Rolle. ... [mehr](#)

Projektleiter: Prof. Dr. Wolfgang Willems

Kooperationen: Prof. Dr. A. Zimmermann

Förderer: DAAD; 01.01.2007 - 31.12.2008

Bilinearformen und Morita-Äquivalenz

Dies ist ein Teilprojekt des Projektes "Bilinearformen und Invarianten in der Darstellungstheorie", für welches PD Dr. Thorsten Holm auf deutscher Seite federführend ist. In Kooperation mit Prof. Dr. A. Zimmermann, Université de Picardie, Amiens, wird untersucht, inwieweit die Morita-Äquivalenz metrische Invarianten respektiert.

Projektleiter: Prof. Dr. Wolfgang Willems

Förderer: Sonstige; 01.01.2005 - 31.12.2008

Representation Theory and Coding Theory

Im Zentrum der Untersuchungen stehen darstellungstheoretische Methoden in der Codierungstheorie. Das Projekt "Representation Theory and Coding Theory" wird bezahlt aus Mitteln des Projektes MTM2004-08219-C02-01. Es läuft über den Zeitraum 2005 bis 2008 in Zusammenarbeit mit der Universidad de Zaragoza. Dort verantwortlich für das Projekt ist Prof. Dr. J. Lafuente.

5. Eigene Kongresse und wissenschaftliche Tagungen

- Prof. Dr. A. Pott: "Kolloquium über Kombinatorik"; Magdeburg; joint with Stefan Felsner; 14.11.-15.11.2008
- Prof. Dr. M. Henk: "Oberwolfach Workshop 'Diskrete Geometrie'"; Oberwolfach; joint with Jiri Matousek, Emo Welzl; 22.09.2008-27.09.2008
- PD Dr. A. Schürmann: "Minisymposium 'Discrete Geometry and Topology at the DMV meeting 2008'"; Erlangen; joint with Frank Lutz; September 2008
- PD Dr. A. Schürmann: "Workshop on Experimentation with construction of and enumeration of optimal geometric structures"; joint with Henry Cohn, Frank Vallentin, Mathieu Dutor Sikiric; Bonn; March 2008
- PD Dr. A. Schürmann: "Workshop Linear and semidefinite programming bounds"; joint with Henry Cohn, Frank Vallentin, Mathieu Dutor Sikiric; Bonn; February 2008
- PD Dr. A. Schürmann: "Trimester Program on Extreme Geometric Structures at the Hausdorff Research Institute for Mathematics"; joint with Henry Cohn, Frank Vallentin, Mathieu Dutor Sikiric; Bonn; February to April 2008

6. Veröffentlichungen

Originalartikel in begutachteten internationalen Zeitschriften

Andresen, Michael; Bräsel, Heidemarie; Mörig, Marc; Tusch, Jan; Werner, Frank; Willenius, Per

Simulated annealing and genetic algorithms for minimizing mean flow time in an open shop

In: Mathematical and computer modelling. - Oxford [u.a.]: Pergamon Press, Bd. 48.2008, 7/8, S. 1279-1293;

[Link unter URL](#)

[Imp.fact.: 0,527]

Bey, Christian

The edge-diametric theorem in Hamming spaces

In: Discrete applied mathematics. - Amsterdam [u.a.]: Elsevier, ISSN 0166-218x, Bd. 156.2008, 9, S. 1510-1517;

[Link unter URL](#)

[Imp.fact.: 0,377]

Bey, Christian; Kyureghyan, Gohar

On boolean functions with the sum of every two of them being bent

In: Designs, codes and cryptography. - Boston, Mass. [u.a.]: Kluwer, Bd. 49.2008, 1/3, S. 341-346; [Link unter URL](#)

[Imp.fact.: 0,681]

Bierbrauer, Jürgen; Kyureghyan, Gohar

Crooked binomials

In: Designs, codes and cryptography. - Boston, Mass. [u.a.]: Kluwer, Bd. 46.2008, 3, S. 269-301; [Link unter URL](#)

[Imp.fact.: 0,637]

Bräsel, Heidemarie; Herms, André; Mörig, Marc; Tautenhahn, Thomas; Tusch, Jan; Werner, Frank

Heuristic constructive algorithms for open shop scheduling to minimize mean flow time

In: European journal of operational research. - Amsterdam: Elsevier, Bd. 189.2008, 3, S. 856-870; [Link unter URL](#)

[Imp.fact.: 1,096]

Canteaut, Anne; Charpin, Pascale; Kyureghyan, Gohar

A new class of monomial bent functions

In: Finite fields and their applications. - Orlando, Fla. [u.a.]: Elsevier, Bd. 14.2008, 1, S. 221-241; [Link unter URL](#)

[Imp.fact.: 0,556]

Charpin, Pascale; Kyureghyan, Gohar

Cubic monomial bent functions - a subclass of [mathcal{M}]

In: Society for Industrial and Applied Mathematics: SIAM journal on discrete mathematics. - Philadelphia, Pa. : Soc., Bd. 22.2008, 2, S. 650-665; [Link unter URL](#)

[Imp.fact.: 0,518]

Henk, Martin; Hernández-Cifre, M. Á.

Notes on the roots of Steiner polynomials

In: Revista matemática iberoamericana. - Madrid, Bd. 24.2008, 2, S. 631-644

[Imp.fact.: 0,886]

Henk, Martin; Hernández Cifre, Maria A.

Intrinsic volumes and successive radii

In: Journal of mathematical analysis and applications. - Amsterdam [u.a.]: Elsevier, ISSN 0022-247x, Bd. 343.2008, 2, S. 733-742; [Link unter URL](#)

[Imp.fact.: 0,872]

Kyureghyan, Gohar

Minimal polynomials of the modified de Bruijn sequences

In: Discrete applied mathematics. - Amsterdam [u.a.]: Elsevier, ISSN 0166-218x, Bd. 156.2008, 9, S. 1549-1553;

[Link unter URL](#)

[Imp.fact.: 0,377]

Schürmann, Achill; Sikiric, Mathieu Dutour; Vallentin, Frank

A generalization of Voronoi's reduction theory and its application

In: Duke mathematical journal. - Durham, NC: Duke Univ. Press, Bd. 142.2008, 1, S. 127-164; [Link unter URL](#)
[Imp.fact.: 1,323]

Willems, Wolfgang; Zimmermann, Alexander

On morita theory for self-dual modules

In: The quarterly journal of mathematics. - Oxford: Oxford Univ. Pr., Bd. 59.2008, insges. 14 S.; [Link unter URL](#)
[Imp.fact.: 0574]

Originalartikel in begutachteten zeitschriftenartigen Reihen

Charpin, Pascale; Kyureghyan, Gohar

On a class of permutation polynomials over F_2

In: Sequences and their applications - SETA 2008. - Berlin [u.a.]: Springer, ISBN 3-540-85911-X, S. 368-376; Lecture notes in computer science; 5203; [Link unter URL](#)
Kongress: SETA; 5 (Lexington, KY): 2008.09.14-18

Göloğlu, Faruk; Pott, Alexander

Results on the crosscorrelation and autocorrelation of sequences

In: Sequences and their applications - SETA 2008. - Berlin [u.a.]: Springer, ISBN 3-540-85911-X, S. 95-105; Lecture notes in computer science; 5203; [Link unter URL](#)
Kongress: SETA; 5 (Lexington, KY): 2008.09.14-18

Kyureghyan, Gohar; Pott, Alexander

Some theorems on planar mappings

In: Arithmetic of finite fields. - Berlin [u.a.]: Springer, ISBN 3-540-69498-6, S. 117-122; Lecture notes in computer science; 5130; [Link unter URL](#), 2008
Kongress: WAIFI; 2 (Siena): 2008.07.06-09

Schmidt, Kai Uwe; Parker, Matthew G. ; Pott, Alexander

Negabent function in the Maiorana-McFarland class

In: Sequences and their applications - SETA 2008. - Berlin [u.a.]: Springer, ISBN 3-540-85911-X, S. 390-402; Lecture notes in computer science; 5203; [Link unter URL](#)
Kongress: SETA; 5 (Lexington, KY): 2008.09.14-18

Wissenschaftliche Monografien

Willems, Wolfgang; García, Ismael Gutiérrez

Una introducción a la criptografía de clave pública. - Barranquilla, Colombia: Ediciones Uninorte; IX, 83 S.: graph. Darst., 2008
[Literaturverz. S. 79 - 80]

Herausgeberschaften

Golomb, Solomon W. ; Parker, Matthew G. ; Winterhof, Arne; Pott, Alexander

Sequences and their applications - SETA 2008 - 5th international conference, Lexington, KY, USA, September 14-18, 2008; proceedings. - Lecture notes in computer science; 5203; Berlin [u.a.]: Springer; XII, 419 S.: graph. Darst.; 235 mm x 155 mm, 2008
Kongress: SETA; 5 (Lexington, KY): 2008.09.14-18
International Conference on Sequences and Their Applications; 5 (Lexington, KY): 2008.09.14-18
[Literaturangaben]

Lehrbücher

Willems, Wolfgang

Codierungstheorie und Kryptographie. - Mathematik kompakt; [Link unter URL](#); Basel [u.a.]: Birkhäuser; VIII, 152 S.:

graph. Darst.; 24 cm, 2008
[Literaturverz. S. [141] - 143]

Buchbeiträge

Andresen, Michael; Bräsel, Heidemarie; Plauschin, Mathias; Werner, Frank

Using simulated annealing for open shop scheduling with sum criteria

In: Simulated annealing. - In-teh, ISBN 978-953-761907-7, S. 49-76, 2008

Helleseht, Tor; Kyureghyan, Gohar; Ness, Geir Jarle; Pott, Alexander

On a family of perfect nonlinear binomials

In: Boolean functions in cryptology and information security. - Amsterdam [u.a.]: IOS Press, ISBN 978-1-586-03878-6, S. 126-138, 2008

Henk, Martin; Ziegler, Günter M.

La congettura di Keplero

In: La matematica; Vol. 2: Problemi e teoremi. - Einaudi, ISBN 88-06-16425-2, 2008

Pott, Alexander

Predigt beim Akademischen Gottesdienst am 15. Januar 2006 in der Wallonerkirche zu Magdeburg

In: Predigten der Magdeburger Akademischen Gottesdienste 2001 bis 2007. - Magdeburg: Univ., Evangel. Hochschulpfarramt, S. 203-212, 2008

Artikel in Kongressbänden

Bouyuklieva, Stefka; Willems, Wolfgang

Notes on automorphisms of extremal codes

In: Algebraic and combinatorial coding theory. - Bulgarian Acad. of Science, S. 40-45, 2008

Kongress: ACCT; 11 (Pamporovo, Bulgaria): 2008.06.16-22

Henk, Martin; Wills, Jörg M.

Minkowski's successive minima

In: Proceedings of the International Conference on Number Theory and Discrete Geometry. - Ramanujan Mathematical Society, S. 129-142, 2008

Habilitationen

Schürmann, Achill

Computational geometry of positive definite quadratic forms - theory algorithms, applications. - Magdeburg, Univ., Fak. für Mathematik, Habil-Schr., 2008; 178 S.: graph. Darst.; 21 cm