INSTITUT FüR ALGEBRA UND GEOMETRIE

Universitätsplatz 2, 39106 Magdeburg
Tel. +49 (0)391 67 18713 / 18321, Fax +49 (0)391 67 11213
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 unterrichtspraktische Untersuchungen zu "Levels of Modeling" (Exponential- und Logarithmusfunktionen als Mathematisierungsmuster) in einem aufgabenbasierten Unterricht in der Sekundarstufe II
- Gestaltungsvarianten für fächerübergreifenden Mathematikunterricht (Platonische Körper in der Kunst, Algebraische und stochastische Aspekte in der Kompositionstechnik ("Mathematisierung in der Musik") ausgewählter Komponisten (Jannis Xennakis, Violetta Dinescu, Tom Johnson))
- Studien zu "Digitale Medien im Unterricht" in Kooperation mit der AG Lehramtsausbildung der Fakultät für Informatik als Planungsgrundlage für eine Verlaufs- und Effektanalyse des Einsatzes vernetzter Medien im Stochastikunterricht in Klasse 7

Diskrete Mathematik

- Untersuchung von binären Sequenzen, von Abbildungen auf endlichen Körpern sowie von Differenzmengen.
  - "almost perfect nonlinear" und "almost bent" Funktionen.
  - Bent-negabent Funktionen.
  - Quadratische Potenzfunktionen.
  - semifields.
  - Partielle Differenzmengen.
  - Äquivalenz von Funktionen.
  - Permutationspolynome.
- Schedulingtheorie
- Kombinatorik

Konvexe und diskrete Geometrie

- Gitterpunkte und das Ehrhart Polynom
- Nullstellen geometrischer Polynome
- Frobenius Problem
- Kompakte Darstellungen spezieller semi-algebraischer Mengen
- Kugelüberdeckungen
- Gemischte Volumina konvexer Körper

Reine Mathematik
- Codierungstheorie
- Extremale Codes
- Automorphismengruppen von Codes
- Involutionen und Kohomologie
- Blocktheorie für verschiedene Primzahlen
- Charaktergrade

4. Forschungsprojekte

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: MTM2007-64504Title: Geometría diferencial y convexa: Problemas variacionales y de optimización Convex and Differential Geometry: Optimization and Variational Problems).Institution: Universidad de MurciaMain researcher: Luis J. Alías LinaresThis is a joint project with the instiute of topolygy and geometry of the universiad murcia.

Projektleiter: Prof. Dr. Florian Heß

Förderer: DAAD; 01.01.2009 - 31.12.2010

Explizite Methoden und Algorithmen in der Zahlentheorie

Im Projekt sollen explizite Methoden und Algorithmen für zahlentheoretische Fragestellungen untersucht werden, welche auch einen Bezug zur Kryptographie aufweisen. Das Augenmerk ist dabei konkret auf die Konstruktion von Zahlkörpern mit gewissen Eigenschaften, die komplexe Multiplikation, Zetafunktionen von Kurven über endlichen Körpern und Paarungen gerichtet.

Das Projekt wird in Kooperation mit David Kohel, Institut de Mathématiques de Luminy, Université de la Mediterranée, Marseille durchgeführt.

Projektleiter: Prof. Dr. Florian Heß

Projektbearbeiter: Dr. Sylla Lesseni

Förderer: EU - Forschungsrahmenprogramm; 01.04.2006 - 31.03.2011

SCIEnce - Symbolic Computation in Europe

Projektziele sind die Vernetzung von Computeralgebrasystemen (darunter GAP, KANT, Maple und MuPAD) sowie Gridcomputing für Computeralgebra. Das Projekt ist ene Integrated Infrastructure Initiative mit acht europäischen Partnern.

Projektleiter: Prof. Dr. Florian Heß

Förderer: EU - Forschungsrahmenprogramm; 01.08.2008 - 31.07.2012

ECRYPT

Das Projekt ist ein Network of Excellence mit einigen europäischen Teilnehmern. Die Zielsetzung des Projekts ist die Förderung von Kollaborationen unter europäischen Forschern im Bereich der Informationssicherheit. Hierzu werden regelmäßig Workshops und Konferenzen organisiert.

Projektleiter: Prof. Dr. Alexander Pott

Projektbearbeiter: Prof. Dr. Alexander Pott, Faruk Göloglu

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: Prof. Dr. Alexander Pott

Projektbearbeiter: Prof. Dr. Alexander Pott, Yue Zhou

Förderer: Sonstige; 01.10.2009 - 30.09.2011

Verallgemeinerte bent Funktionen

Die Menge der verallgemeinerten bent-Funktionen GF(q^n) \rightarrow GF(q^m), m<n bildet eine Halbordnung . Ziel des Projektes ist es, diese partiell geordnete Menge explizit zu bestimmen (zumindest für kleine Körper q und n, d. h. kleine Zahlen.

Projektleiter: Prof. Dr. Wolfgang Willems

Projektbearbeiter: Anton Malevich

Förderer: Land (Sachsen-Anhalt); 01.09.2008 - 31.05.2010

Existenz und Konstruktion extremaler Codes

Extremale Codes kann es nur bis zu einer Länge von 3964 geben. Bekannt sind nur Codes bis zur Länge 156. Es klafft also eine große Lücke zwischen der theoretisch bewiesenen Schranke und dem, was wir konstruieren können. Aufgabe des Projektes ist es, weitere Klarheit zu schaffen; insbesondere extremale Codes mit zusätzlichen Eigenschaften, etwa QR, zu klassifizieren.

Projektleiter: Prof. Dr. Wolfgang Willems

Projektbearbeiter: Yanjun Liu

Förderer: Sonstige; 01.10.2009 - 30.09.2010

Grade von irreduziblen Charakteren

In der modularen Darstellungstheorie sind bis heute viele tiefliegende Fragen, die teilweise bereits Richard Brauer 1963 gestellt hat, offen. So weiß man über die Grade der irreduziblen Brauer-Charaktere von endlichen Gruppen recht weinig. Im Projekt solllen Beweise oder auch weitere Evidenz für bekannte Vermutungen über die Grade der irreduziblen Brauer-Charaktere erbracht werden.

Projektleiter: Prof. Dr. Wolfgang Willems

Projektbearbeiter: Javier de la Cruz

Förderer: DAAD; 01.04.2009 - 31.03.2011

Automorphismen von extremalen Codes

Extremale Codes haben optimale Eigenschaften hinsichtlich der Fehlerkorrektur bei der Datenübertragung. Bis heute sind jedoch nur ganz wenige solcher Codes bekannt. Mögliche Automorphismengruppen könnten beim Aufsuchen neuer Codes entscheidend helfen.
Im Projekt wird nach einer möglichen Automorphismengruppe eines extremalen Codes der Länge 120 gesucht.

5. Eigene Kongresse und wissenschaftliche Tagungen

- Prof. Dr. W. Willems: "Optimal codes and related topics", Sixth Int. Workshop, 16.06.-22.06.2009, Varna, Bulgarien
- Prof. Dr. A. Pott: "Kolloquium über Kombinatorik"; Magdeburg; joint with Stefan Felsner; 13.11.-14.11.2009
- Prof. Dr. A. Pott: "Finite Fields", Dublin; joint with Gary McGuire; 13.07.-17.07.2009

6. Veröffentlichungen

Originalartikel in begutachteten internationalen Zeitschriften

Aliev, Iskander; Henk, Martin
Integer knapsacks - average behavior of the Frobenius numbers
In: Mathematics of operations research. - Linthicum, Md. : Inst., ISSN 0364-765x, Bd. 34.2009, 3, S. 698-705; **Link unter URL**
[Imp.fact.: 1,086]

Charpin, Pascale; Kyureghyan, Gohar
When goes G(x)+GTr(H(x)) permute F p n?
In: Finite fields and their applications. - Orlando, Fla. [u.a.]: Elsevier, Bd. 15.2009, 5, S. 615-632; **Link unter URL**
[Imp.fact.: 0,609]

Henk, Martin; Averkov, Gennadiy
Three-dimensional polyhedra can be described by three polynomial inequalities
In: Discrete & computational geometry. - New York, NY: Springer, Bd. 42.2009, 2, S. 166-186; **Link unter URL**
[Imp.fact.: 0,754]

Henk, Martin; Hernandez Cifre, Maria
Successive minima and radii
In: Canadian mathematical bulletin. - Toronto: Univ. of Toronto Press, Bd. 52.2009, 3, S. 380-388

Henk, Martin; Tagami, Makoto
Lower bounds on the coefficients of ehrhart polynomials
In: European journal of combinatorics. - Amsterdam: Elsevier, Bd. 30.2009, 1, S. 70-83; **Link unter URL**
[Imp.fact.: 0,678]

Martinez-Pérez, Conchita; Willems, Wolfgang
The trivial intersection problem for characters of principal indecomposable modules
In: Advances in mathematics. - Amsterdam [u.a.]: Elsevier, Bd. 222.2009, 4, S. 1197-1219; **Link unter URL**
[Imp.fact.: 1,280]

Zha, Zhengbang; Kyureghyan, Gohar; Wang, Xueli
Perfect nonlinear binomials and their semifields
In: Finite fields and their applications. - Orlando, Fla. [u.a.]: Elsevier, Bd. 15.2009, 2, S. 125-133; **Link unter URL**
[Imp.fact.: 0,453]

Originalartikel in begutachteten zeitschriftenartigen Reihen

Bouyuklieva, Stefka; Malevich, Anton; Willems, Wolfgang
On extremal codes with automorphisms
In: International Workshop on Optimal Codes and Related Topics. - Varna, S. 26-31, 2009
Kongress: International Workshop on Optimal Codes and Related Topics; 6 (Varna): 2009.06.16-22

Buchbeiträge

Edel, Yves; Pott, Alexander
On the equivalence of nonlinear functions
In: Enhancing cryptographic primitives with techniques from error correcting codes. - Amsterdam: IOS, ISBN 978-1-607-50002-5, S. 87-103; NATO Science for Peace and Security Series - D: Information and Communication Security; 23; **Link unter URL**, 2009
Kongress: NATO Advanced Research Workshop on Enhancing Crytographic Primitives with Techniques from Error Correcting Codes; (Veliko Tarnovo, Bulgaria): 2008.10.06-09

Kyureghyan, Gohar; Tan, Yin
On a family of planar mappings
In: Enhancing cryptographic primitives with techniques from error correcting codes. - Amsterdam: IOS, ISBN 978-1-607-50002-5, S. 175-178; NATO Science for Peace and Security Series - D: Information and Communication Security; 23; **Link unter URL**, 2009
Kongress: NATO Advanced Research Workshop on Enhancing Crytographic Primitives with Techniques from Error Correcting Codes; (Veliko Tarnovo, Bulgaria): 2008.10.06-09

Leneke, Brigitte
Aufgaben variieren - Mathematik erfinden und erleben
In: Mathemagische Momente. - Berlin: Cornelsen, ISBN 978-3-06-001185-8, S. 112-119, 2009