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

Dr. Gohar Kyureghyan

2. Hochschullehrer

Prof. Dr. Martin Henk

Prof. Dr. Herbert Henning

Prof. Dr. Florian Heß (bis 30.09.2010)

Prof. Dr. Gohar Kyureghyan (Vertretungsprof. ab 01.10.2010)

Prof. Dr. Alexander Pott

Prof. Dr. Wolfgang Willems

3. Forschungsprofil

Didaktik der Mathematik

- Planung, Durchführung, Verlaufs- und Effektanalyse eines Unterrichtsversuches zum Einsatz digitaler Lernwerkzeuge als Experiment
- Untersuchung von Individualisierungskonzepten bei der Gestaltung multimedialen Lernens
- Herausbildung methodischer Handlungskompetenzen bei der Planung, Durchführung und Auswertung digitalen Mathematikunterrichts
- Untersuchung zur Behandlung graphentheoretischer Elemente im Mathematikunterricht
- Untersuchung zum entdeckenden Lernen an offenen Aufgaben und offenen Unterrichtsformen

Diskrete Mathematik

- Untersuchung von binären Sequenzen, von Abbildungen auf endlichen Körpern sowie von Differenzmengen, Studium von projektiven Ebenen
- "almost perfect nonlinear" und "almost bent" Funktionen
- Bent-negabent Funktionen
- Quadratische Potenzfunktionen
- Quadratische Potenzfunktionen
- semifields
- Partielle Differenzmengen
- Äquivalenz von Funktionen
- Permutationspolynome
- Projektive Ebenen und semifields

Konvexe und diskrete Geometrie

- Geometrie der Zahlen
- Extremalprobleme in der Konvexgeometrie
- Nullstellen geometrischer Polynome
- Packungen konvexer Körper
- Gemischte Volumina konvexer Körper
- Ganzzahlige Optimierung

Reine Mathematik

- Codierungstheorie (Extremale Codes, Automorphismen)
- Darstellungstheorie (Involutionen und Kohomologie, Höhere Frobenius-Schur-Indikatoren)

4. Kooperationen

- Cardiff University
- Centre National de la Recherche Scientifique, Paris
- CODES, INRIA, Frankreich
- Computational Mathematics Group, Universität Kassel, Kassel
- CWI, Amsterdam
- Michigan Technology, Houghton
- Prof. Dr. A. Zimmermann
- Research Institute for Symbolic Computation, Linz
- The Centre for Interdisciplinary Research in Computational Algebra (University of St Andrews, Scotland),
- Universidad de Barranquilla, Kolumbien
- Universidad de Murcia
- Universität Bergen
- Universität Siegen
- Universitdad de Zaragoza
- University Dublin
- University of Crete
- University of Ghent
- ZIB Berlin

5. Forschungsprojekte

Projektleiter: Prof. Dr. Alexander Pott

Projektbearbeiter: John Dillon, Yves Edel, Alexander Pott

Kooperationen: John Dillon, Yves Edel

Förderer: Haushalt; 01.01.2010 - 31.12.2011

New constructions of planar and almost perfect nonlinear functions

Relative difference sets and similar structures (planar functions, almost perfect nonlinear functions) can be modified using a certain switching construction ("project-and-lift"). This idea is due to John Dillon, Yves Edel and Alexander Pott. In this project, we will investigate the strength but also the limitations of the switching idea.

Projektleiter: Prof. Dr. Alexander Pott

Projektbearbeiter: Yves Edel, Alexander Pott

Kooperationen: Yves Edel

Förderer: Haushalt; 01.01.2010 - 31.12.2010

Semifields and APN functions

Almost perfect nonlinear functions (APN) may be viewed as the even characteristic generalization of planar functions. Planar functions provide us with a rich combinatorial (projective planes) and algebraic (commutative semifields) structure. In this project, we investigate possible generalizations of semifields to the APN situation.

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 - 15.12.2011

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

Höhere Frobenius-Schur-Indikatoren geben Aufschluss über die Struktur gewisser Permutationsmoduln. Für p = 2 weiß man relativ viel, p \not= 2 steht im Zentrum der Untersuchungen. In der Blocktheorie wird eine Klassifikation sämtlicher endlicher Gruppen mit genau zwei Blöcken angestrebt.

Projektleiter: Prof. Dr. Wolfgang Willems

Projektbearbeiter: Javier de la Cruz

Förderer: DAAD; 01.04.2009 - 31.03.2012

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 Zentrum der Untersuchungen stehen die Automorphismengruppen der extremalen Codes der Länge 72 und 96.

Projektleiter: Prof. Dr. Martin Henk

Projektbearbeiter: Dipl.-Math. Carsten Thiel; Prof. Dr. Martin Henk

Förderer: Haushalt; 01.05.2010 - 30.04.2013

Adelische Geometrie der Zahlen

Es werden klassische Ungleichungen und Fragestellungen aus dem Bereich der Geometrie der Zahlen in beliebigen Zahlenkörpern untersucht, z.B., Gitterpunktungleichungen und sukzessive Minima, Packungsprobleme, Blichfeldt-Typ Ungleichungen, usw.

Projektleiter: Prof. Dr. Martin Henk

Projektbearbeiter: Dr. Eugenia Saorin Gomez; Prof. Dr. Martin Henk

Kooperationen: Cardiff University, Prof. Dr. Maria A. Hernandez Cifre (Universidad de Murcia)

Förderer: Sonstige; 01.01.2010 - 31.12.2012

Convex and Differential Geometry: variational and optimization problems

Federführend bei diesem Projekt ist die Universität Murcia, Spain, Departamento de Matematicas, vertreten durch Prof. Luis Jose Alias Linares. Gesamtes Fördervolumen ca. 126.000 Euro. Im Rahmen dieses Projektes werden Extermalprobleme der Konvex- und Differentialgeometrie in Kooperation mit der spanischen Seite untersucht. Im Vordergrund stehen hier die Minkowskischen Quermaßintegrale glatter Körper und Flächen. Referenz: MTM2009-10418 Spanish Ministery of Science and Innovation.

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

Kooperationen: Prof. Dr. Maria A. Hernandez Cifre (Universidad de Murcia)

Förderer: Haushalt; 01.04.2009 - 31.03.2014

Steiner-Polynom und Gitterpunkte

Basierend auf Ungleichungen von Blichfeldt, Hadwiger und Wills werden Verbindungen zwischen dem Steiner Polynom und der Anzahl der Gitterpunkte in konvexen Körpern untersucht. Im Zentrum steht dabei die Frage nach oberen Schranken für die Gitterpunktanzahl mittels eines geeigneten gewichteten Steiner-Polynoms.

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

Kooperationen: Centre National de la Recherche Scientifique, Paris, Computational Mathematics Group, Universität Kassel, Kassel, Research Institute for Symbolic Computation, Linz, The Centre for Interdisciplinary Research in Computational Algebra (University of St Andrews, Scotland),

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.

6. Eigene Kongresse, wissenschaftliche Tagungen und Exponate auf Messen

- Prof. Dr. M. Henk: Workshop ``Radii of convex bodies'', (jointly with Rene Brandenberg), Magdeburg, 15.03. - 17.03.2010
- Prof. Dr. A. Pott: "Sequences and Their Applications - SETA 2010", 6th International Conference, Paris (France), 13.09.-17.09.2010

7. Veröffentlichungen

Originalartikel in begutachteten internationalen Zeitschriften

Aliev, Iskander; Henk, Martin
Feasibility of integer knapsacks
In: SIAM journal on optimization. - Philadelphia, Pa. : SIAM, Bd. 20.2010, 6, S. 2978-2993; **Link unter URL**; 2010
[Imp.fact.: 1,429]

Bouyuklieva, Stefka; Malevich, Anton; Willems, Wolfgang
Automorphisms of extremal self-dual codes
In: Institute of Electrical and Electronics Engineers: IEEE transactions on information theory. - Piscataway, NJ: IEEE, Bd. 56.2010, 5, S. 2091-2096; **Link unter URL**; 2010
[Imp.fact.: 2,357]

Henk, Martin; Linke, Eva; Wills, Jörg M.
Minimal zonotopes containing the crosspolytope
In: Linear algebra and its applications. - New York, NY: American Elsevier Publ., Bd. 432.2010, 11, S. 2942-2952; **Link unter URL**; 2010
[Imp.fact.: 1,073]

Tan, Yin; Pott, Alexander; Feng, Tao
Strongly regular graphs associated with ternary bent functions
In: Journal of combinatorial theory. - Orlando [u.a.]: Elsevier, Bd. 117.2010, 6, S. 668-682; **Link unter URL**; 2010
[Imp.fact.: 0,783]

Tiep, Pham Huu; Willems, Wolfgang
Brauer characters of prime power degrees and conjugacy classes of prime power lengths
In: Algebra colloquium. - Singapore [u.a.]: World Scientific, Bd. 17.2010, 4, S. 541-548; 2010
[Imp.fact.: 0,380]

Originalartikel in begutachteten zeitschriftenartigen Reihen

Charpin, Pascale; Kyureghyan, Gohar
Monomial functions with linear structure and permutation polynomials
In: Finite fields. - Providence, RI: American Math. Soc., ISBN 978-0-8218-4786-2, S. 99-112; Contemporary mathematics; 518, 2010
Kongress: International Conference on Finite Fields and Applications; 9 (Dublin): 2009.07.13-17; 2010

Chee, Yeow Meng; Tan, Yin; Zhou, Yue
Almost p-Ary Perfect Sequences
In: Sequences and their applications - SETA 2010. - Berlin [u.a.]: Springer, ISBN 3-642-15873-0, S. 399-415; Lecture notes in computer science; 6338; **Link unter URL**
Kongress: SETA; 6 (Paris): 2010.09.13-17; 2010

Pott, Alexander; Zhou, Yue
Switching construction of planar functions on finite fields
In: Arithmetic of finite fields. - Berlin [u.a.]: Springer, ISBN 3-642-13796-2, S. 135-150; Lecture notes in computer science; 6087; **Link unter URL**, 2010
Kongress: WAIFI; 3 (Istanbul): 2010.06.27-30; 2010

Wissenschaftliche Monografien

Eid, Wolfram; Biallas, Ingrid; Hilmer, Sybille; Liesenberg, Günter; Messner, Ardito; Szebrat, Heike
Arbeitsheft Mathematik Na klar! 5 Sachsen-Anhalt Sekundarschule. - Berlin: DUDEN PAETEC; 56 S., ISBN 978-3-8355-1140-8, 2010; 2010

Eid, Wolfram; Biallas, Ingrid; Hilmer, Sybille; Liesenberg, Günter; Messner, Ardito; Szebrat, Heike
Arbeitsheft Mathematik Na klar! 6 Sachsen-Anhalt Sekundarschule. - Berlin: DUDEN PAETEC; 56 S., ISBN 978-3-8355-1143-9, 2010; 2010

Eid, Wolfram; Biallas, Ingrid; Hilmer, Sybille; Liesenberg, Günter; Messner, Ardito; Szebrat, Heike
Lehrermaterial Mathematik Na klar! 5 Sachsen-Anhalt Sekundarschule. - Berlin: DUDEN PAETEC, ISBN 978-3-8355-1139-2, 2010; 2010

Eid, Wolfram; Biallas, Ingrid; Hilmer, Sybille; Liesenberg, Günter; Messner, Ardito; Szebrat, Heike
Lehrermaterial Mathematik Na klar! 6 Sachsen-Anhalt Sekundarschule. - Berlin: DUDEN PAETEC, ISBN 978-3-8355-1142-2, 2010; 2010

Eid, Wolfram; Biallas, Ingrid; Hilmer, Sybille; Liesenberg, Günter; Messner, Ardito; Szebrat, Heike
Lehrermaterial Mathematik Na klar! 7 Sachsen-Anhalt Sekundarschule. - Berlin: DUDEN PAETEC; 127 S., ISBN 978-3-8355-1145-3, 2010; 2010

Eid, Wolfram; Biallas, Ingrid; Hilmer, Sybille; Liesenberg, Günter; Messner, Ardito; Szebrat, Heike; Unger, Michael
Arbeitsheft Mathematik Na klar! 7 Sachsen-Anhalt Sekundarschule. - Berlin: DUDEN PAETEC; 56 S., ISBN 978-3-8355-1146-0, 2010; 2010

Herausgeberschaften

Carlet, Claude; Pott, Alexander
Sequences and their applications - SETA 2010 - 6th international conference, Paris, France, September 13-17, 2010; proceedings. - Lecture notes in computer science; 6338; Berlin [u.a.]: Springer; X, 463 S., ISBN 3642158730, 2010
Kongress: SETA; 6 (Paris): 2010.09.13-17
International Conference on Sequences and Their Applications; 6 (Paris): 2010.09.13-17
[Literaturangaben]; 2010

Lehrbücher

Huppert, Bertram; Willems, Wolfgang
Lineare Algebra - mit zahlreichen Anwendungen in Kryptographie, Codierungstheorie, Mathematischer Physik und Stochastischen Prozessen. - Aus dem Programm Lineare Algebra; **Link unter URL**; Wiesbaden: Vieweg + Teubner; XV, 619 S., ISBN 978-3-8348-1296-
[Literaturverz. S. [607] - 608]; 2010

Willems, Wolfgang; García, Ismael Gutiérrez
Una introducción a la criptografía de clave pública. - Barranquilla, Colombia: Ediciones Uninorte; XI, 88 S., ISBN 978-958-825263-6, 2010; 2010

Buchbeiträge

Eid, Wolfram
Niveaubestimmende Aufgaben - (nicht nur) ein Mittel zur Implementierung curricularer Vorgaben
In: Beiträge zum Mathematikunterricht 2010; Bd. 1:. - Münster: WTM, Verl. für Wiss. Texte und Medien, S. 265-268
Kongress: Tagung für Didaktik der Mathematik; (München): 2010.03.08-12; 2010

Eid, Wolfram; Pruzina, Manfred
Zeichnerisches Darstellen im Mathematikunterricht
In: Materialien zum Erprobungslehrplan Sekundarschule, Fach Mathematik, IFG Mathematik; **Abstract unter URL**, 2010; 2010

Leneke, Brigitte
Kompetenzentwicklung mit graphikfähigen Taschenrechnern im Mathematikunterricht
In: Mathematische Kompetenzen entwickeln und erfassen. - Hildesheim [u.a.]: Franzbecker, ISBN 978-3-88120-803-1, S. 75-86, 2010; 2010

Willems, Wolfgang
On binary self-dual extremal codes
In: 19th International Symposium on Mathematical Theory of Networks and Systems, MTNS 2010. - Budapest, ISBN 978-963-311-370-7, S. 303-304
Kongress: MTNS 2010; 19 (Budapest, Hungary): 2010.07.05-09; 2010

Habilitationen

Kyureghyan, Gohar
Optimal mappings of finite fields. - Magdeburg, Univ., Fak. für Mathematik, Kumulative Habil.-Schr., 2010; Getr. Zählung: graph. Darst.; 30 cm
[Die Habil.-Schr. beinhaltet eine Sammlung von Veröffentlichungen des Autors]; 2010