

# **Forschungsbericht 2005**

**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@mathematik.uni-magdeburg.de oder  
jeannette.polte@mathematik.uni-magdeburg.de

### 1. Leitung

Prof. Dr. Martin Henk (geschäftsführender Leiter bis 11/2005)  
Prof. Dr. Herbert Henning (bis 11/2005)  
Prof. Dr. Alexander Pott (geschäftsführender Leiter ab 12/2005)  
Prof. Dr. Wolfgang Willems (ab 12/2005)  
Jun.-Prof. Dr. Christian Bey  
Dr. Achill Schürmann (ab 12/2005)

### 2. Hochschullehrer

Juniorprofessor Dr. Christian Bey  
Prof. Dr. Jürgen Bierbrauer (Vertretungsprofessor WS 2004/05)  
Prof. Dr. Heidemarie Bräsel  
Prof. Dr. Martin Henk  
Prof. Dr. Herbert Henning  
PD Dr. Thorsten Holm (z. Z. beurlaubt)  
Prof. Dr. Alexander Pott  
Prof. Dr. Wolfgang Willems

### 3. Forschungsprofil

#### Didaktik der Mathematik

- Verlaufs- und Effektanalyse zur Umsetzung von 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" unter dem Aspekt Bewertung und Kontrolle

#### Diskrete Mathematik

- Untersuchung von binären Sequenzen, von Abbildungen auf endlichen Körpern sowie von Differenzmengen. Im Berichtszeitraum wurden insbesondere folgende wichtige Ergebnisse erzielt:
  - Charakterisierung von "Crooked binomials"
  - Bestimmung der Kreuzkorrelation diverser perfekter Sequenzen
  - Konstruktion neuer "almost perfect nonlinear" und "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"

### **Geometrie**

- Approximierbarkeit von reellen Zahlen durch rationale Zahlen mit beschränktem Nenner
- Gitterpunkteigenschaften konvexer Körper
- Nullstellen des Erhart-Polynoms
- Extremale Gitter
- Kugelüberdeckungen
- Klassifikation perfekter Gitter
- Gleichseitige Mengen in normierten Räumen

### **Kombinatorik**

- Diskrete isoperimetrische und -diametrische Probleme
- Kombinatorik partieller Ordnungen

### **Reine Mathematik**

- Codierungstheorie
  - Konstruktion optimaler Codes
  - selbstduale Codes
  - Decodierfehlerwahrscheinlichkeiten
- Gruppen- und Darstellungstheorie
  - Charaktergrade und Klassenlängen
  - Quadratische Geometrien und Involutionen
  - Blocktheorie
  - Dualität

## **4. Forschungsprojekte**

**Projektleiter:** Jun. Prof. Dr. Christian Bey

**Förderer:** Haushalt; 01.10.2004 - 30.09.2006

### **Polynomiale LYM Eigenschaften partieller Ordnungen**

Im Projekt soll untersucht werden, inwieweit die vor kurzem entdeckte polynomiale LYM Eigenschaft des Booleschen Verbandes für allgemeine partielle Ordnungen gilt. Beziehungen zur Spernertheorie sind herauszuarbeiten.

---

**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:** Bettina Matzke  
**Kooperationen:** Dipl. Math. Bettina Matzke, Dipl. Math. Hartwig Bosse, CWI, Amsterdam,  
Prof. Dr. Martin Grötschel, ZIB Berlin  
**Förderer:** Haushalt; 01.03.2003 - 28.02.2006

#### **Darstellung von Polyedern durch Polynome**

Basierend auf einem klassischen Resultat aus der reellen algebraischen Geometrie werden konstruktive Darstellungen von Polyedern durch wenige Polynomgleichungen gesucht. Die Anzahl der Ungleichungen hängt dabei nur von der Dimension und nicht von der kombinatorischen Struktur des Polyeders ab.

---

**Projektleiter:** Prof. Dr. Alexander Pott  
**Kooperationen:** Universität Bergen  
**Förderer:** DAAD; 01.01.2004 - 31.12.2005

#### **Kodierungstheorie und Kryptografie**

In dem Projekt werden zusammen mit Wissenschaftlern der Universität Bergen (Norwegen) diverse Probleme aus der Kodierungstheorie und Kryptografie bearbeitet. Insbesondere

- "Fingerprinting"
- fast perfekte und perfekte Funktionen auf endlichen Körpern
- zyklische Differenzmengen

---

**Projektleiter:** Prof. Dr. Alexander Pott  
**Projektbearbeiter:** Prof. Dr. Alexander Pott, Lilya Budaghyan  
**Förderer:** Land (Sachsen-Anhalt/ohne Gutachtersystem); 01.04.2003 - 30.03.2006

#### **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:** Dr. Achill Schürmann  
**Kooperationen:** Frank Vallentin (Jerusalem / Amsterdam)  
**Förderer:** DFG; 01.05.2005 - 30.04.2007

#### **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:** Universidad de Zaragoza  
**Förderer:** Sonstige; 01.01.2005 - 31.12.2008

### **Representation Theory and Coding Theory**

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. W. Willems: Workshop "Algebraic Coding Theory"; 02.03. - 03.03.2005; zusammen mit Prof. Zimmermann in Amiens (Frankreich)
- Prof. Dr. M. Henk: Oberwolfach workshop "Discrete Geometry"; joint with Jiri Matousek, Emo Welzl; 10.04. - 16.04.2005
- Prof. Dr. M. Henk: Workshop "Inside the Cube: Algebra, Combinatorics and Geometry"; Magdeburg; joint with Jesus de Loera; 01.07. - 03.07.2005
- Prof. Dr. M. Henk: Euroconference in Mathematics on Crete "Algebraic and Geometric Combinatorics"; joint with Christos Athanasiadis, Victor Batyrev, Dimitrios Dais, Francesco Santos; Anogia; 20.08. - 26.08.2005
- Prof. Dr. A. Pott: European Conference on Combinatorics (Programm committee); Berlin; 05. - 10.09.2005
- Dr. A. Schürmann: Oberwolfachseminar "Sphere packings: Exceptional structures and relations to other fields"; joint with Henry Cohn, Robert Griess; 20.11. - 26.11.2005

## **6. Veröffentlichungen**

### ***Originalartikel in internationalen Zeitschriften***

**Baicheva, Tsonka (ext.); Bouyukliev, Iliya (ext.); Dodunekov, Stefan (ext.); Willems, Wolfgang**

Teaching linear codes.

In: *Mathematica Balkanica* [Sofia] 19(2005), Nr. 1/2, S. 3 - 16

**Betke, Ulrich (ext.); Schürmann, Achill**

Lattice of optimal finite lattice packings.

In: *Monatshefte für Mathematik* [Wien] 144(2005), Nr. 1, [Elektronische Ressource] [Imp.fact.: 0.348]

**Bey, Christian**

On cross-intersecting families of sets.

In: *Graphs and combinatorics* [Tokyo] 21(2005), Nr. 2, S. 161 - 168 [Imp.fact.: 0.235]

**Bey, Christian**

Polynomial LYM inequalities.

In: *Combinatorica* [Budapest] 25(2005), Nr. 1, S. 19 - 38

[Imp.fact.: 0.388]

**Bey, Christian**

Remarks on an edge isoperimetric problem.

In: Electronic notes in discrete mathematics [Amsterdam] 21(2005), S. 243 - 244; [Elektronische Ressource]

**Bey, Christian**

The edge-diametric theorem in hamming spaces.

In: Electronic notes in discrete mathematics [Amsterdam] 21(2005), S. 245 - 248; [Elektronische Ressource]

**Bosse, Hartwig (ext.); Groetschel, Martin (ext.); Henk, Martin**

Polynomial inequalities representing polyhedra.

In: Mathematical programming [Berlin] 103(2005), Nr. 1, S. 35 - 44, [Elektronische Ressource]  
[Imp.fact.: 1.016]

**Henk, Martin**

Free planes in lattice sphere packings.

In: Advances in geometry [Berlin] 5(2005), S. 137 - 144  
[Imp.fact.: 0.282]

**Kyureghyan, Gohar**

Minimal polynomials of the modified de Bruijn sequences.

In: Electronic notes in discrete mathematics [Amsterdam] 21(2005), S. 333 - 336; [Elektronische Ressource]

**Schürmann, Achill; Vallentin, Frank (ext.)**

Local covering optimality of lattices: leech lattice versus root lattice E8.

In: International mathematics research notices: IMRN [New York, NY](2005), Nr. 32, S. 1937 - 1955  
[Imp.fact.: 0.906]

**Willems, Wolfgang**

On degrees of irreducible Brauer characters.

In: Transactions of the American Mathematical Society [Providence, RI] 357(2005), Nr. 6, S. 2379 - 2387  
[Imp.fact.: 0.839]

**Originalartikel in nationalen Zeitschriften**

**Herget, Wilfried (ext.); Leneke, Brigitte; Henning, Herbert; Eid, Wolfram; Malitte, Elvira (ext.); Richter, Karin (ext.); Schuster, Eva (ext.)**

Mathematik-Kompetenzen in Klasse 7: Leistungsstudie MUSA in Sachsen-Anhalt.

In: Der Mathematikunterricht: MU [Seelze-Velber] 51(2005), Nr. 2/3, S. 93 - 107

**Schürmann, Achill; Dutour, Mathieu (ext.); Vallentin, Frank (ext.)**

On lattice sphere packings and coverings.

In: Oberwolfach Reports [Zürich] 2(2005), Nr. 2, Report 17, [S. 51 - 53]

### **Originalartikel in zeitschriftenartigen Reihen**

#### **Bey, Christian**

Quadratic LYM inequalities.

In: Felsner, Stefan (Hrsg.): EuroComb 2005 (European conference on combinatorics, graph theory and applications Berlin September 5-9 2005). - conference proceedings. Nancy: LORIA, 2005, S. 37 - 40 (DMTCS proceedings series Vol. AE)

#### **Eun, Yu-Chang (ext.); Song, Hong-Yeop (ext.); Kyureghyan, Gohar**

One-error linear complexity over  $F_p$  of Sidelnikov sequences.

In: Helleseth, Tor (Hrsg.); Sarwate, Dilip (Hrsg.); ... (Hrsg.): Sequences and their applications, SETA 2004 (Third international conference, Seoul, Korea, October, 24 - 28, 2004). - revised selected papers. Berlin: Springer, 2005, S. 154 - 165 (Lecture notes in computer science 3486)

#### **Hertel, Doreen**

Cross-correlation properties of perfect binary sequences.

In: Helleseth, Tor (Hrsg.); Sarwate, Dilip (Hrsg.); ... (Hrsg.): Sequences and their applications, SETA 2004 (Third international conference, Seoul, Korea, October, 24 - 28, 2004). - revised selected papers. Berlin: Springer, 2005, S. 208 - 219 (Lecture notes in computer science 3486)

#### **Kyureghyan, Gohar**

Crooked maps in finite fields.

In: Felsner, Stefan (Hrsg.): EuroComb 2005 (European conference on combinatorics, graph theory and applications Berlin September 5-9 2005). - conference proceedings. Nancy: LORIA, 2005, S. 167 - 170 (DMTCS proceedings series Vol. AE)

#### **Leneke, Brigitte**

Einführung in die Graphentheorie: mit Graphen kürzeste Wege finden; (ab 10. Schuljahr).

In: Hopp, Reinhard (Red.): RAAbits: Impulse und Materialien für die kreative Unterrichtsgestaltung; Mathematik, Sekundarstufe I. Bd. 1. 4. Ausg. Stuttgart: Raabe, 2005, Kapitel I/F (Nachschlagen - Finden). - Loseblattausg., Stand: März 2005

#### **Pott, Alexander**

Group algebras and correlation immune functions.

In: Helleseth, Tor (Hrsg.); Sarwate, Dilip (Hrsg.); ... (Hrsg.): Sequences and their applications, SETA 2004 (Third international conference, Seoul, Korea, October, 24 - 28, 2004). - revised selected papers. Berlin: Springer, 2005, S. 437 - 450 (Lecture notes in computer science 3486)

### **Buchbeiträge (einschließlich Lehrbuchbeiträge)**

#### **Fack, Veerle (ext.); Bouyukliev, I. (ext.); Willems, Wolfgang; Winne, J. (ext.)**

Projective two-weight codes with small parameters and their corresponding graphs.

In: Bulgarian Academy of Sciences, Institute of Mathematics and Informatics (Veranst.): Optimal codes and related topics (Fourth international workshop Pamporova, Bulgaria June 17-23, 2005). - proceedings. Sofia: Bulgaria Academy of Sciences, 2005, S. 139 - 145

**Willems, Wolfgang**

On the automorphism group of a binary self-dual doubly-even [72, 36, 16] code, part II.

In: Bulgarian Academy of Sciences, Institute of Mathematics and Informatics (Veranst.): Optimal codes and related topics (Fourth international workshop Pamporova, Bulgaria June 17-23, 2005). - proceedings. Sofia: Bulgaria Academy of Sciences, 2005, S. 283 - 285

**Artikel in Kongreßbänden**

**Henk, Martin**

Finite and infinite lattice packings.

In: Banna, Eiichi (Hrsg.): Sphere packings (COE workshop Fukuoka, Japan 1 - 5 November 2004). proceedings. Fukuoka, 2005, S. 80 - 91

**Kyureghyan, Gohar**

Differentially affine maps.

In: Charpin, Pascale (Hrsg.); Ytrehus, Oyvind (Hrsg.): Coding and cryptography, WCC '2005 (International workshop Bergen, Norway, March 14 - 18, 2005). - proceedings. Paris, 2005, S. 296 - 305

**Pott, Alexander; Bugaghyan, Lilya; Carlet, Claude (ext.)**

New constructions of almost bent and almost perfect nonlinear polynomials.

In: Charpin, Pascale (Hrsg.); Ytrehus, Oyvind (Hrsg.): Coding and cryptography, WCC '2005 (international workshop Bergen, Norway, March 14 - 18, 2005). - proceedings. Paris, 2005, S. 306 - 315

**Schürmann, Achill; Vallentin, Frank (ext.)**

Methods in the local theory of packing and covering lattice.

In: Banna, Eiichi (Hrsg.): Sphere packings (COE workshop Fukuoka, Japan 1 - 5 November 2004). proceedings. Fukuoka, 2005, S. 122 - 136

**Hochschulschriften**

**Budaghyan, Lilya**

The equivalence of almost bent and almost perfect nonlinear functions and their generalizations. 2005, XII, 77 S. Magdeburg, Univ., Fak. für Mathematik, Diss., 2005